Global Insights in Artificial Intelligence and Computing

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

Intersection of AI and Cybersecurity: Protecting Healthcare Data in a Connected World

Ghaith Alomari[1*]

[1]Chicago state university, USA

[1]galomari@csu.edu

open access

Corresponding Author

Ghaith Alomari
galomari@csu.edu

Article History:
Submitted: 13-01-2025
Accepted: 16-02-2025
Published: 21-02-2025

Keywords:
AI, Cybersecurity in healthcare, data protection, threat introduction, compliance, HIPAA, GDPR, ethic, Openness, Bias, temporal.

ABSTRACT

The release of Artificial Intelligence in healthcare cybersecurity is innovative as it safeguards the patient's data, recognizes threats while its occurrence and address cyber threats. However, its adoption raises concern with the following issues and concerns relating to data privacy, the law and ethics. In the following review, the different ways that AI enhances healthcare cybersecurity threat enumeration, data safeguarding, and reaction are examined. The principles of HIPAA and GDPR as well as the remaining principles concerning legislative requirements are also introduced in order to establish the knowledge on how healthcare organizations are required to keep with the rules of privacy and security of data. Some of the ethical concerns which arise when it comes to the issue of use of artificial intelligence in a healthcare organization include; In addition, the review outlines emerging AI solutions two of which are efficient but safeguard privacy preservation methods which are federated learning and differential privacy. Thus while relying on growth potential of AI in the enhancement of health sector cybersecurity: The implementation should be done carefully to respect patients' rights and privacy, Shield laws and ethical standards.

INTRODUCTION

Digital technologies is not randomly integrating the healthcare sector as it seeks to improve on patient experiences, organization functionality and decision making. At the core of this effort is the integration of artificial intelligence which is revolutionizing so many fields including diagnosis, treatment, follow up and even administration. More health information is being created and addressed daily as AI integration advances in the healthcare sector, and this increases the degree of cyber risk.

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

When the networks, devices, and cloud platforms are becoming involved in the healthcare systems; the cyber threats and unauthorized access to the information, in general, rose dramatically [1]. Healthcare sector that heavily rely on large amount of data, and become prone to cyber threats. The information that can be stored in healthcare systems including heath information like records, treatment documents and diagnostic and patient details are among the most sensitive information that should not fall into the wrong hands of hackers hence accorded the name 'virtue'. Any get to such data or any form of infringement of it is dangerous and may result in numerous impacts for example identity thefts and scams to a compromise of the patient safe. Not only should one mention external threats; internal threats include poor access controls, non-informed staff, and old systems are also to blame for many connections' problems in the healthcare structures [2].

AI has thereby emerged as a solution that helps to lessen these difficulties. AI can simulate a large amount of data, recognize deviant patterns and future security risks, therefore the AI efficiency in improving cybersecurity in the healthcare industry. There is a possibility to study tendencies in the network traffic, reveal the suspicious activity of users or even an attempt at hacker attack, response within a few moments thanks to the dynamically changing AI systems. Moreover, by using AI, tasks to which earlier, great load was imposed on IT groups such as data encryption, risk evaluation, and compliance reports, and enhancing the stability of the systems [3].

But, and this is the point which we would like to stress, an increase in the use of AI in the sphere of healthcare has expanded the number of factors to take into consideration about cybersecurity. This is especially the case as expanding usage of AI systems attests new risks tied to data privacy, initiatives involving the sharing personal health information, and new forms of risk to address. As the AI algorithms becomes even more developed the aspects which need to be considered are transparency, accountability and adherence to regulatory norms of healthcare. AI therefore when used together with cybersecurity and information access within the sphere of healthcare therefore presents both opportunity and risks that should be well thought out. Much as this review seeks to find out how AI is impacting the cybersecurity in health care, the technologies that are used, the problems that have occurred and the solutions that have in turn emerged. It is therefore important to look at current development and development in prospect that AI has in improving security of health care data with provision of ethical use [4].

THE ROLE OF AI IN HEALTHCARE

Artificial intelligence is an emerging technology that is relatively new but taking root rapidly in healthcare services with the potential to enhance the quality in many areas of the discipline. ML and DL are enhancing dimensions of accuracy, velocity, and operations of health care services. From

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

diagnosis and therapeutic planning, through patients monitoring and even administrative activities AI is currently engaged in the process of reforming system performance in delivery of healthcare services with positive impacts on patients [5].

AI Applications in Healthcare: DIAGNOSIS is perhaps the most developed area of AI in healthcare that is best understood. Machine learning has been effective in the reading of the image and, if doctors use X-ray, MRIs, CT scans, they will be able to diagnose early the diseases. AI systems are able to identify certain parts of medical data that human vision may not be able to notice hence end up diagnosing more accurate results than machines. For example, the use of the artificial intelligent models has been used in diseases such as cancer diseases, heart diseases, and neurological diseases and so on. Another central area where AI is really revolutionary is the field of individualized therapeutic plans [6]. AI can benefit the patients by studying the information about the patient's health condition such as the family and genetic history, and life history of the patient before administering them with medics. With the help of the concept of predictive analytics, AI models can also indicate why those patients are at high risk of developing certain diseases in the future and help come up with prevention strategies. This is perhaps the reason why the results for treatments vary from patient to patient so that the actual tumor patients are protected from adverse reactions while the effectiveness of treatments is improved [7].

AI in Patient Monitoring and Management: AI also includes patient observation, particularly of managing chronic conditions as well. They include the smart devices that include artificial intelligence that can track patients' status in warding off their physical outlook that may be constantly changing to include pulse rates, blood pressure and glucose levels at any one time day or night. These devices provide timely information for this reason the providers are able to manage the sufferers off location and act if necessary [8]. This type of telemedicine is highly useful for chronic diseases and helps prevent readmissions in diabetic, hypertensive, and COPD patients improving the quality of life of patients it has treated. AI is also affecting the business aspects of the health care domain; Most of the health care institutions are applying AI for some features such as, fixing schedules, charging and distribution of the health care resources among others. AI in healthcare is developed from NLP to identify potential patterns from the large datasets such as EHRs for decision making, for enhancing operational effectiveness of the health care sector, and for CAD of the caregivers [9].

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

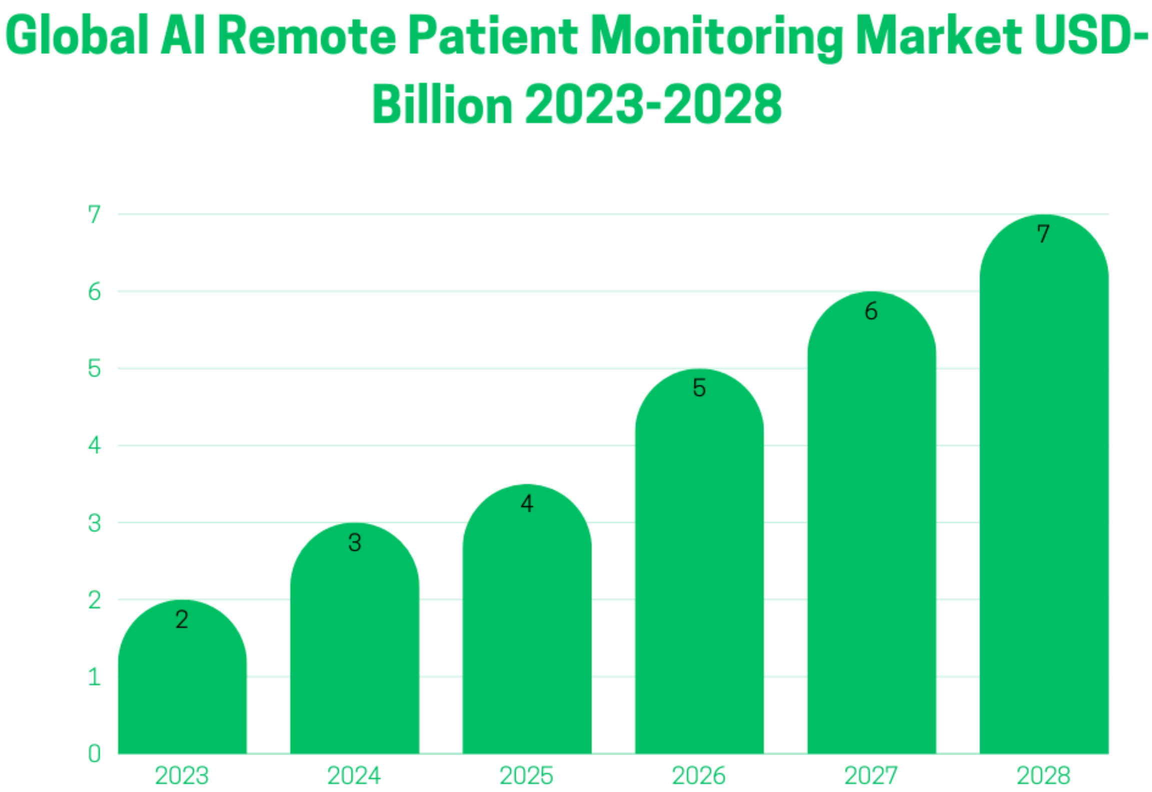

Figure: 1 showing global remote patient monitoring market

Data Processing and Management Using AI: Another application includes Big Data Management- an area where an assignment that is ideal for healthcare, if we consider the help of AI. Electronic health records, diagnosis imaging, genetic data and health monitoring all generate big data. AI can indeed be employed in a way that It will be able to receive, process, analyze and synthesise encouraging amounts of data to feed the knowledge in diagnosable treating and in the advancement of clinical research [10]. Moreover, such algorithms can fast and more effectively search for relations and links of IPR that may not of clear for human understanding which is very important for the population health knowledge and medical science [11].

Benefits of AI in Improving Healthcare Outcomes: The integration of AI in to health systems has endless benefits in terms of the overall functionality of a proper healthcare organization. By following different types of automation methods it is possible to free up large amount of time of different healthcare professions for more patients and delicate oriented assignments. Similar to human employees, no fatigue is experienced by KAMAI, the AI-derived stations and thus they can provide patients' supervision throughout the night and day, identifying any variations from the standard, and documentation. This lead to high operating efficiency, short time waiting, more access to health facilities especially in the few and or no facilities within the region. AI data processing also may

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

identify areas of service shortage and section resource deployment for efficiency [12]. This should enable patients receive treatment at the right time as well as possible improved patient outcomes over groups of patients. It also has enormous potential of reducing the healthcare costs since it has the potential of making enhanced diagnosis and minimizing probabilities of erroneous treatments and practical errors in the same manner which can also eliminate costs formalities. AI is an additional game for healthcare since it brings fresh concepts into typical issues. It is changing diagnosis, outcome planning, patient tracking and organizational management. However, recent development in AI has arisen that requires sobriety and integration of the principles of data protection, ethics or regulations that are supposed to safeguard AI practice in the health care systems [13].

The changed use of information technology and the networking of most systems in the medical sector has taken the opportunity and outlook of patients to another level. But if we look at these advancements then the severe issues of cyber security are in front of us now that healthcare data is under threat. HCA maintaining organizations are at a high risk given the type of information that the organizations deal with together with the complex setting in which the organizations are placed. These are the stringencies that healthcare institutions have to consider, namely; Data privacy, meeting the legal requirements and not to be involved in cyber hazards [14].

ASSORTED TYPES OF RISKS WITH CONCERNING HEALTH CARE INFORMATION

Some of the busiest and valuable information in the world include; personal health records (PHRs), medical histories, diagnostic results and treatment. It makes the healthcare institution to be vulnerable to the attacks of cyber criminals. Consequently, a cyber-attacks on a healthcare organization can be categorized into; Data breaches, Ransom Ware Attacks, phishing and Insider threats [15].

Data Breaches: Disadvantages of the Advantages Potential beneficiaries' data was exposed at Schools' staff for unauthorized access and data containing identifiable information could be used to perpetrate identity theft. Patient's personal health information is violated by parties such as delinquent parties, who might sell them in black markets or indulge in schemes. In other instances, they are due to nefarious access to the clinical health system or leveraging vulnerabilities inherent in the healthcare IT landscape or by-passing inept security controls [16].

Ransom ware Attacks: Ransom ware as can be seen has been quite prevalent in the health care industry as an attack type. Here for an instance a software targets the data of an organization and threatens the world that they cannot be used without making a payment. The healthcare sector is still a favorite area of attack because this segment is deemed to be a zero-day for days or weeks, given the nature of important work within the sector and because it is within these accounts that the attackers are likely to receive the ransom for regaining control [17].

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

Phishing and Social Engineering: Phishing emails and applying social engineering to the employees of the healthcare organization are among the most active actions of cybercriminals to get the rightful access to login credentials and other sensitive information. The hackers may claim to be a member of some organization or clinics just in order to gain access to patients' record and make initiating of unamiable nature [18].

Insider Threats: Healthcare organizations are also at risk for the very reason that the attacker might be one of its insiders. Medical information can also be misused through the prejudicial action from employees, contractors and other personnel with allowed access into the healthcare facilities. Thus, owing to its very nature inherent in its purpose and identity as either reckless or malicious the insider threat is a challenge to counter in its endeavor to safeguard patient data from being compromised [19].

CHALLENGES IMPACT REGULATORY AS WELL AS COMPLIANCE OF THE ORGANIZATIONS

It is thus important for the healthcare organizations to engage in a struggle with a mind-boggling set of the formal standards that has been designed to safeguard the patient's data. Most laws such as HIPAA in USA or the GDPR in EU have laws that regulate the disclosure of patient's information [20].

HIPAA Compliance: Security of the patient's health information is required from healthcare facilities through compliance with rules of HIPAA. This include; Risk assessment which is done periodically, use of passwords to the information and encryption of the information and restriction of the information access. HIPAA violation has an associated penalty financially and it also exposes that an organization has not complied with the rules [21].

GDPR: Another regulation which offers privacy and data protection regulation for the healthcare institution that operates in EU or manage the data of EU persons is the GDPR. The GDRP also regulates the storage and access of data besides data processing and analyzes the rights of an individual. Failure to observe the provisions of GDPR is punishable by law and also organizations vulnerable to a bad reputation. Core technologies like EHR, cloud computing, and connected medical devices increase the size of threat along with the progressive integration of healthcare systems [22]. The conventional use of IoT devices Such as wrist band health monitors, connected health equipment the following risk factors are brought in. If left insecure, these devices lead to security threat to keys as there is high possibility the attackers may seek control over the important data alongside manipulate severe medical procedures.

Besides that, the infrastructure of starting health care industries may not be standard; therefore, they

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

are vulnerable to cyber hackers. The practice of many hospitals and clinics continuing to use devices and programs that are no longer the most recent to the marketplace means that their aesthetic contemporary security design can be lacking and they cannot be easily updated or repaired [23]. That is why this creates enormous cybersecurity threats waiting to be used by the offenders. There are also potential threats within the healthcare organizations as continues next. Some external risks such as lack of staff consideration for cyber threats and risks, weakness in passwords and staff management, inadequate training in staff also pose a lot of danger to an organization since they expose the organization to risks like data breach and cyber-attack. Staff members who have not been trained on how to report cases of phishing incidences, or how to handle sensitive information might be the cause of a cyber-threat [24].

Therefore, enhancing the human factor or the people component suggests that that very concept must continue pushing for a dependence on training to refine the health care employees to areas of vulnerability. The students also established that when there is regular cyber security training and the use of phishing, the employees get to be informed of various threats and how they can protect the firm's information. Medical cyber security is very challenging and on-going process. As healthcare organizations continue to remain competitive and offer care in more efficient ways, they should strengthen their information technology security mechanisms to ensure patient data complies with laid down standards [25]. This means that managing the ever increasing threat of cyber-attacks is not a one fit for all situation, rather it is the correct tactic that involve, Access Control Measures, Replacement of old structures, training the employees and incorporating use of artificial intelligence/ machine learning to aid in early threat and risk identification. It is a principle to protect the privacy of patients and also secrets of the entire healthcare industry.

ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY FOR HEALTH CARE SYSTEM

Obviously AI has come out as a blessing for uplifting cybersecurity solutions in different sectors and the health care sector got introduced with same too. With the increase in the value of information assets and the increasing occurrence of high risk threat levels, AI has been found to be invaluable for enhancing the security of heath care organizations. The implementation of cyber security solutions which uses Artificial Intelligence makes it efficient to detect, protect and avoid cyber risks as it will create secure Health care frameworks for patients' privacy and trust [26].

AI-Enhanced Threat Detection and Prevention: Of all the advantages the role of AI the most helpful to healthcare cybersecurity is the ability to address threats in real time. Past measures aimed to fight cyber threats are insufficiently protective since they include signature-based detection, where

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

threats are identified by their pattern or signature. However, potential acts of cybercriminals are always present, and they develop new forms of threats that can overwhelm traditional systems. As an element of AI integration, ML is meant for identifying those patterns and outliers within large datasets that are unnoticed by conventional means at all [27]. For instance, AI systems are trained to read, in real-time, the traffic on a network and look for 'forbidden patterns' as attempts of access, leakage of data or strange behavior of the system. These AI models always receive new data for processing and can learn from them, hence, the chances of the success noticed by the AI models of such attack will not happen again. Further, AI can categorize these threats based to their likely negative effect on the healthcare organization, and as such determine the threats to work on first [28].

AI for Data Encryption and Protection: Safety concern plays a big focusing device of health care industry since record and identity of patients and their health information and treatment history are very sensitive. First of all, healthcare must involve AI in a process that can justify the encryption of storing and transmitting health information. The methods of encrypting data for a long time have always been with the use of predetermined procedures and sometimes involved human beings —this means that there can be an element of error or that the process will be slowed down. In contrast, encryption applications with uses of AI has the capacity to advance in tandem with the type of new threats to the extent of preserving information in a given period [29]. For instance, an AI system will discover that some data is being read or written and it automatically encrypts the data. Besides, AI has the potential of supplementing key management best practice in a way that the encrypted keys are sufficiently managed and protected from an attacker who specifically focuses on the weakness of the key management [30].

AI in Incident Response and Recovery: Regarding how the health care organizations handle the cybersecurity threats, there is also adoption of new changes by the use of AI. When handling breach or attack, reliance of traditional paper based processes for managing the incident is extremely costly, this means that the time taken before addressing the problem is longer and therefore the risk exposure level is higher and the longer it takes to take option the higher the amount of loss that has been incurred. AI, however, has the ability to enhance the amount of time devoted to identification and responses to such incidents by handling some of the fundamental elements of the incident process [31]. In fact, while using the AI technologies, it is possible to promptly define the kind of attack, the range of the problem and perform the above Scripts to counteract the problem for instance by isolating the affected systems in the network, or blocking the relevant IP addresses, or beginning back up processes and the like, As for the forensics, it will also take less time to use AI and find out how and which of the vulnerabilities was exploited [32].

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

AI in Compliance Monitoring: This privacy legislation includes the Health Insurance Portability and Accountability Act (FHIPAA) for health care organization in USA and General Data Protection Regulation (GDPR) for EU. These regulations detail specifically how it can and must be used, and protected, and in what ways it has to be done. AI technology is capable of automating some of the compliance monitoring processes like auditing and logging and reporting thus helping organizations to maintain compliance with these regulations while Oregon Unemployment Tax [33]. In residual control, an AI system can run through the operations of the healthcare systems and arrest any compliance related concern or risk signal in a real time basis. For example, AI can monitor the use of patient records and give information on those using records and those who have legal right to use records to dismiss the remaining unqualified users. The other is the advantage of incorporating the new style of security in as prescribed in the compliance standard and in compliance with the ever emerging security threats.

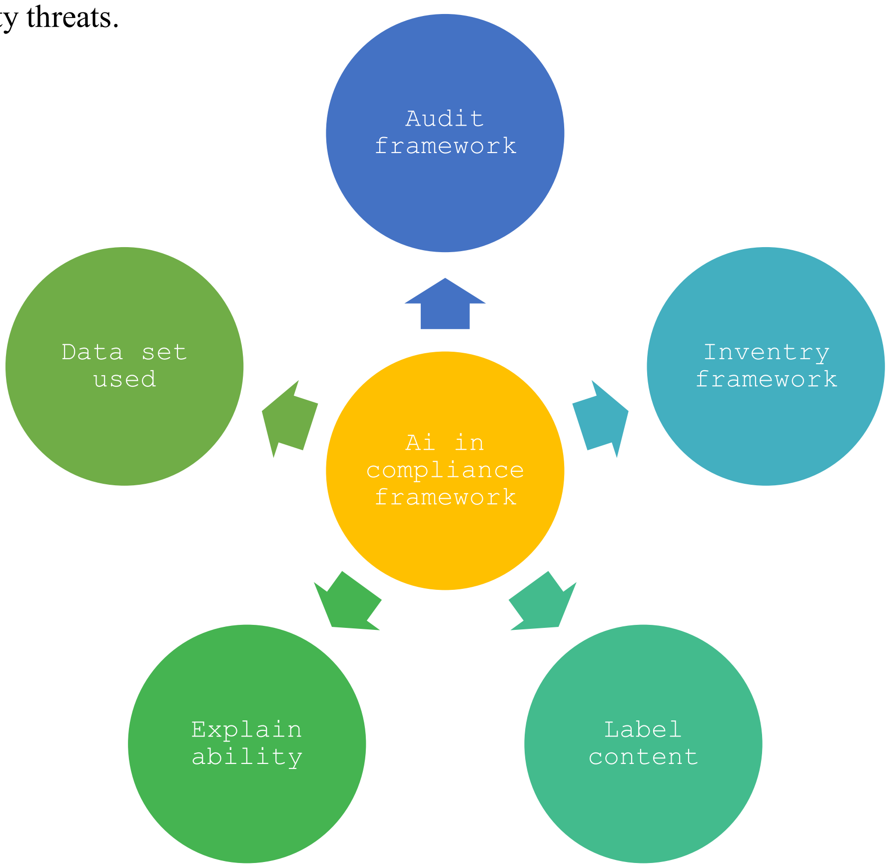

Figure: 2 showing AI in compliance framework

Case Studies of AI in Healthcare Cybersecurity: For now, some of the lights in the healthcare organizations have been shed through applying AI in their crypto SicherheitAufbau programmer. For instance, the AI robotics popular in identification of ransom ware is disastrous in the health departments has been embraced. Any time an administrator discovers a pattern in network, an AI system is synchronizable to alert the administrators once encryption activities signs of ransom ware

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

attack are identifying, and the system counters by containing the attack. Apart from the above mentioned areas related to cybersecurity, AI has been applied for enhancing protection for medical devices very vulnerable to cyber risks because of their central role in the delivery of health services. Anticipative safety can also be assured because the AI based security tools can observe the devices' behavior, variations and intervene to notify the concerned recipients of imminent dangers that are potentially fatal to the patient's lives [34].

What we mean by AI is actually redesigning the shape of cybersecurity and the way in which the healthcare organizations safeguard PHI and avert IIAs.' As AI strengthens comprehensibility of threats, management of risks, response to incidents, and compliance factors, it strengthens the general security environment of the healthcare network systems thereby providing the system a greater leverage against Cyber attackers [35]. This is promising, given the increasing interest of many healthcare organizations in the digital sphere; the future role of artificial intelligence in cybersecurity will be a critical factor in the preservation of patient privacy and protection of structures and the actualities of health care systems in this increasingly interconnected world.

AI OPTIMIZATION IN AS MUCH AS DATA PROTECTION

Since one of the actors in the enhancement of the healthcare system is AI, most displays of how data is processed point to poor privacy. But, actual in Apply AI means that through processing large amounts of data AI rationalize patient care, improve flow, and reduce costs. They pointed out that despite admitting that with the increased deviance of applying AI in health care that there is a core concern with acknowledgment of patient data which is sensitive in various health care systems [36].

AI and Data Privacy Concerns: All healthcare data is inevitably personal; therefore, this information has to be protected to maintain patient's trust in addition to legal requirements like HIPAA in USA or GDPR in EU. There are some AI systems based on the ML and DL that critically depend on big data since true algorithms are callable only using numerous amounts of parameters. Such data sets include a patient history, genetic information or data on the kind of treatment it has given to its patient which are if not well managed, pose great risks. The final concern that people have concerning the adoption of employment of Artificial Intelligence in healthcare organizations is on the question of security [37]. It is thus not necessarily hard for authorship, ownership, possession of the patient data to be breached particularly if these models of artificial intelligence were trained with this data and used it in their models. For instance, an AI algorithm in the healthcare organization may leak, individual identifiers such as the patient's health information due to poor encryption. But the cloud services which are including the AI solutions has its own issue because data is stored in the cloud and everyone such as a cybercriminal or other person can access the data [38].

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

Data Anonymization and Encryption: These privacy concerns can be met in the common type of data masking where the entire PII are 'eliminated' before the data is used by the AI. This means that patient's identity does not allow the patient's identity to be hidden but, at the same time, the AI system can be trained by the patient's information. Yet, anonymization is not very effective because at some point in the future anonymity can be reversed as the AI procedures are improved on constantly. But for this purpose, there are other more sophisticated techniques like data masking or differential privacy which go a step further and hide even more attributes along with usability. They have come up with other two other crucial improvements to the data privacy; one of them is encryption [39]. Information that can be recorded for patients', or used in others ways that involve storage and transfer of the same can actually be encoded in a manner, which does not allow other parties access to it. Something that contributed to this is to ensure that if it got with wrong people, it remain as information that cannot be used. In addition, since they are AI encryption devices, they have the ability to adapt the encryption type for any of these threats; these AI encryption devices offer a real-time encryption service which represents an improved circumstance over traditional encryption types [40].

AI's Impact on Informed Consent: Also, another obvious or fundamental factor that have safeguarded data privacy in areas of 'the health care system impacted by artificial intelligence is consent. To the patient's case, what will be done with the information, to whom it will be disclosed, and what might occur are especially relevant? Since such processes are actually complex in some of the existing current AI systems, it is quite difficult to explain them to many of the patients. Indeed it has been argued that current models especially under the Deep learning class of models are notorious for being difficult to query that means one cannot ask the model to explain the basis of its conclusion that it presented hence the black box title. The four stated factors can give rise to workarounds – such as developing the opacity in uses of data not so readily reversible and thus, must raise ethical issues to consent. To this, the healthcare organizations require to keep in mind that they must also explain to the patients on how the 'AI systems' are employed and the processes used to ensure data security [41]. This would include made accessible relevant and understandable information about the advantages or disadvantages of the use of AI in the healthcare industry and also the option given to the patient on whether his data could be used for AI processing.

Regulatory Compliance and Ethical Considerations: But the efficiency of the AI methods and absolutely safe safeguard of the data, demonstrated in the state and non-state practices, does need compliance with the healthcare rules and regulations and recognition of the ethical norms. For instance, the GDPR enjoins the processing of data with the following conditions: It must be relevant, compatible with the purpose for which it is processed in a manner that does not harm the data subject's

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

interests and rights and the party that process the data must provide an explanation about that [42]. The regulation also has the data minimization principle which also contends that only limited amount of personal data should be processed. Healthcare organization should also apply these ethical principles as AI systems adopt their systems. This means for instance checking that the strategy does not have prejudices inbuilt into it and does not has slipped in sources for biased treatment of some people. AI use and design require a lot of consideration and immense precaution when handling the patient's information should not be overlooked [43].

The Future of AI and Data Privacy: Though it was demonstrated that AI helps to improve the efficiency of activities in different fields, its scale together with data protection will always remain a challenge in the healthcare sector. Thus, the use of a privacy-preserving A methodology such as federated learning and securemulti-party computation therefore provides a reasonable solution because data remains decentralized yet AI can be trained. These approaches minimize privacy risks up to a level where no raw data is ever forwarded although AI systems use analysis of big data. As laudable, the role of AI in healthcare is there is need to ensure data does not become a victim of the powerful tool. By establishing evidence of the four significant approaches to data anonymisation, encryption, openness and meeting the present law, the AI assists healthcare organizations to improve the treatment of patients with the protection of patient data. As AI continues to advance in the future as will the technology pertaining to data privacy, healthcare systems will have to be alert and apt to counter the challenges that may come as a result of theory avidity of the benefits that stem from the integration of AI in the host organization [44].

ISSUES OF LEGAL AND ETHICAL CHARACTER IN RELATION TO ARTIFICIAL INTELLIGENCE TECHNOLOGY IN THE FIELD OF CYBERSECURITY OF HEALTH CARE

The applying of AI in the healthcare cybersecurity nave legal and moral issues that healthcare managers have to address in order to secure the patients' information and meet the legal obligations. Other strengths of Application of AI other include enhanced ability in detecting and handle cyber risks; they enhance data protection and handling measures and response; however in the health industry, it is all about following the set rules or regulation and also good ethics. The escalating influx of regulations and ethical standards is making it crucial for healthcare organizations to identify better how to compete with the rising trend in a way that will allow them to meet patients' expectations in AI powered cybersecurity safely [45].

Regulatory Frameworks in Healthcare Cybersecurity: Health information security and confidentiality have been provided by relevant organizations in various nations. Among these, the

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

most famous two are Health Insurance Portability and Accountability Act (HIPAA) in United States and General Data Protection Regulation (GDPR) in EU. All the above regulations' aims to protect patient information and compliance with adequate security measures that can prevent or reduce the breach of patient data [46].

HIPAA Compliance: HIPAA mandates that within he United States, particular conditions must protect patient health information in a healthcare organization; the administrative, physical, and technical. The first security priorities should therefore be achieved to aid in the protection of PHI while allowing audit trails through the AI driven cybersecurity solutions. Furthermore, when it comes to the patient's data AI systems must follow the data minimalism, according to which only the person who needs to see the data for specific purpose such as a treatment or invoicing should have access to it [47].

GDPR Compliance: The GDPR is the data protection law in EU, which provides the framework of data privacy as a legal instrument. The GDPR prohibits collection or processing of any of the patient's information without their permission and the patient is allowed to withdraw such permission at any given time. The concept of artificial intelligent enabled cybersecurity solutions has to ensure that patient information is not a violated GDPR especially on issues to do with data subject's right to access, right to erasure and right to portability. They also should not incorporate imprudent assumptions that might lead to discriminations against the provisions of the GDPR principles of fairness and transparency [48]. The deployment of artificial intelligence in the area of healthcare cybersecurity presents several unique and significant ethical concern, particularly in the area of transparency, the possibility of the fair decision as well as the accountability for same. This is so because most of the AI systems are incurred with mechanism such as machine learning and deep-learning and therefore the decision making by the system is in the black-box means. From ethical considerations, this lack of openness is not desirable, more so where an AI system is applied in threat detection, or in coming up with the security architectures that will impact a patient or individual's data or care [49].

Transparency and Accountability: Appropriate ethical use of AI requires organizations to inform the public how the used artificial intelligence systems arrive at their decisions. This means that for the healthcare organization AI-based cybersecurity solution has to be transparent and comprehensible why certain security mechanisms are applied to stakeholders like patients and providers and must also be easily understandable by the regulators. This applies to reasonable levels of responsibility for consequences arising from the malfunction of an AI system or its failure to recognize that it has been hacked or that there is an ongoing cyber-attack and also the responsibility that organizations have to

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

be able to identify the inputs to an AI system that led to the production of the decisions that caused the security breaches [50].

Bias and Fairness: Therefore, the utilization of AI systems is capable of becoming an enhancement of prejudices if the AI systems feature data from earlier days as their input. For example, if an AI model has to focus on cybersecurity threats, it could end up mistaking certain behaviors or grouping them as dangerous leading to conduct and user monitoring more significantly than necessary leading to over-ministration of certain demographics [51]. Such concerns in the subject, within the context of healthcare industry might raise issues to do with data protection and to do with patient's right, leading to discrimination of the patient by health care givers. To resolve such issues, the medical centers should have AI software to go through the diagnostics for bias and the same dataset that contain samples resembling population should be used for model training [52].

Informed Consent: Other ethical principles of the AI use in healthcare cybersecurity are also such as informed consent: It also implies that patient ought to be told on how the information will be utilized particularly w.r.t to artificial intelligence in protecting it. This disclosure is very essential as patient has to get benefits from any technology and the technologies that is going to be used on the patient. This is even worse when the AI systems are applied within an even bigger health care system where it hard to know how your information is being processed [53]. Yet, as the decades progress the regulation and ethical concerns appeared as new standards and best practices are set concerning the application of AI for dealing with healthcare cybersecurity. With the aim of raising accountability, reliability and trust of the end user, organizations are exploring on how to produce XAI or explainable AI that should enable these intelligent models to be understood easily by the human handlers and the machines [54].

Additionally, several healthcare/ cybersecurity bodies active in AI capacity are calling on organizations to adopt privacy preserving techniques including federated learning and differential privacy that allow organizations to train their AI models without acquiring or sharing patient-level data. The use of such practices is not unlawful, or in violation of privacy and data protection laws and is also sensitive to ethical questions as to use of data. An issue that relates to the regulation and the competent and ethical application of artificial intelligence in healthcare cybersecurity is an issue that deserves more study [55]. More, healthcare organizations have to take into account the potentiality of the AI application in processes of cybersecurity and in patients' therapy on the one hand, and in maintaining patients' information security, legal regulations, and ethical norms on the other. If healthcare systems will follow such regulation and guidelines as HIPAA and GDPR, they will stick to the fair and transparent approach, and use the privacy-friendly approach of AI possibilities, they

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

can achieve all the positivity's of AI use, and exclude the negative impact, which ignores the rights of patients and their data protection.

CONCLUSION

AI integration to the management of healthcare cybersecurity is an innovative trend that enhances security to data and increases the threat detection threshold while also enhancing the operation effectiveness. But anything that brings advancement in the facet of health care has its drawbacks and the application of artificial intelligence has its shortcomings also, specifically for the problems in the integration of the privacy and ethical concerns that are attached to the identification and handling of the patient's health informatics data. Finally, it is clear how through the understanding of how the integration of AI may offer competitive benefits in cyber protection by recognizing threats and encrypting information in real time, thus initiating quick action to address episodes and enforce compliance. All of these capabilities also enhance the security structure of these healthcare enterprises and PHI thus are useful in establishing patient confidence as well as meeting the legal necessities.

Firstly, AI is able to improve the level of cybersecurity, while, on the other hand, the costs are the regulative and the ethical concerns. Any attempt at acquiring, evaluating, and archiving patient information due to systems such as HIPAA and GDPR creates a stipulation that the institutionalization of AI in healthcare organizations face a challenge of complexity when it comes to compliance. Another aspect that we consider ethical is the issue of clarity and responsibility, proportionality and impartiality to overcome the problem of justice and oe nails where the latter has to be impartial in arriving at the recommendation. These problems cannot be solved otherwise other than through an application of multiple methods.. First, regulatory compliance with data protection and privacy must be achieved these are mandatory rules for all applied AI solutions in healthcare organizations. Second, the norms of ethical behavior should be chosen Tai: in order.

AI systems do not practice bias in any way; the information regarding them and every AI model is public; and AI systems are humane. However, to address this challenge likely to be encountered when applying AI in the cyber-security processes to resolve the privacy problem, Federated learning, and data Differential privacy techniques can be applied. There is great promise yet unfulfilled for AI in the arena of healthcare cybersecurity in the future, but this has to be addressed in a way which pays respect to the patient data as well as the rules of realism, virtue, efficiency, and law. Should such issues be faced, healthcare organizations will be in a position to implement AI to make health-care safer as per data security and privacy of the patients. It is therefore probably going to be a progressive process to observe and adjust those strategies which are going to aid properly utilize AI technology in the cybersecurity affairs of healthcare.

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

REFERENCES

[1]. Alsadie D. Artificial intelligence techniques for securing fog computing environments: trends, challenges, and future directions. IEEE Access. 2024 Sep 19.

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

[3]. Arefin S, Simcox M. AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity. International Business Research. 2024 Nov;17(6):1-74.

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

[5]. Harnessing Artificial Intelligence to Drive Global Sustainability: Insights Ahead of SAC 2024 in Kuala Lumpur. Digitalization & Sustainability Review, 4(1), 16-29. https://upright.pub/index.php/dsr/article/view/161

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

[7]. Neoaz N, Bacha A, Khan M, Sherani AM, Shah HH, Abid N, Amin MH. AI in Motion: Securing the Future of Healthcare and Mobility through Cybersecurity. Asian Journal of Engineering, Social and Health. 2025 Jan 29;4(1):176-92.

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

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

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

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

[12]. Shahana A, Hasan R, Farabi SF, Akter J, Mahmud MA, Johora FT, Suzer G. AI-driven cybersecurity: Balancing advancements and safeguards. Journal of Computer Science and Technology Studies. 2024 May 10;6(2):76-85.

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

[13]. García, N. C., Libu, M., Ravinder, D. (2019). Energy Autonomous Electronic Skin. NPJ Flexible Electronics, 3(1). https://doi.org/10.1038/s41528-018-0045-x

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

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

[16]. Gummadi, J. C. S., Thompson, C. R., Boinapalli, N. R., Talla, R. R., & Narsina, D. (2021). Robotics and Algorithmic Trading: A New Era in Stock Market Trend Analysis. Global Disclosure of Economics and Business, 10(2), 129-140. https://doi.org/10.18034/gdeb.v10i2.769

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

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

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

[20]. Awad AI, Babu A, Barka E, Shuaib K. AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications. 2024 May 1;82:103748.

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

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

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

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

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

[26]. Ghimire, P., Kim, K., & Acharya, M. (2023). Generative AI in the Construction Industry: Opportunities & Challenges. arXiv preprint arXiv:2310.04427.

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

[28]. Al-Mhdawi, M. K. S., Qazi, A., Alzarrad, A., Dacre, N., Rahimian, F., Buniya, M. K., & Zhang, H. (2023). Expert Evaluation of ChatGPT Performance for Risk Management Process Based on ISO 31000 Standard. Available at SSRN 4504409

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

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

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

[32]. Vemprala, S., Bonatti, R., Bucker, A., & Kapoor, A. (2023). Chatgpt for robotics: Design principles and model abilities. Microsoft Auton. Syst. Robot. Res, 2, 20

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

[34]. Ofusori L, Bokaba T, Mhlongo S. Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Applied Artificial Intelligence. 2024 Dec 31;38(1):2439609.

[35]. Shah HH, Lodhi SK. AI in Personalized Medicine: Tailoring Treatment Plans Based on Individual Patient Data. Global Trends in Science and Technology. 2025 Jan 24;1(1):15-29.

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

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

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

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

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

[40]. Khan M, Bacha A. Neural Pathways to Emotional Wellness: Merging AI-Driven VPSYC Systems with EEG and Facial Recognition. Global Trends in Science and Technology. 2025 Jan 26; 1(1):53-62.

[41]. Nasir S, Hussain HK, Hussain I. Active Learning Enhanced Neural Networks for Aerodynamics Design in Military and Civil Aviation. International Journal of Multidisciplinary Sciences and Arts. 3(4):152-61.Z.

[42]. Jabbarova K. Ai and cybersecurity-new threats and opportunities. Journal of Research Administration. 2023;5(2):5955-66.

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

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

[45]. Adeyeye OJ, Akanbi I, Emeteveke I, Emehin O. Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection. International Journal of Research and Publication and Reviews. 2024;5(10):3208-23.

[46]. Dabić M, Maley JF, Švarc J, Poček J. Future of digital work: Challenges for sustainable human resources management. Journal of Innovation & Knowledge 2023; 8:100353. https://doi.org/https://doi.org/10.1016/j.jik.2023.100353

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

[48]. Saheb, T., Dehghani, M., & Saheb, T. (2022). Artificial intelligence for sustainable energy: A contextual topic modeling and content analysis. Sustainable Computing: Informatics and Systems, 35. https://doi.org/10.1016/j.suscom.2022.100699

[49]. Adio-moses, D., & Asaolu, O. S. (2016). Artificial intelligence for sustainable development of intelligent building. Research Gate, 9(February

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.37-56

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

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

[52]. Ma S, Huang Y, Cai W, Leng J, Xu J. Integrated sustainable benchmark based on edge-cloud cooperation and big data analytics for energy-intensive manufacturing industries. Journal of Manufacturing Systems 2024; 74:1037–56. https://doi.org/https://doi.org/10.1016/j.jmsy.2024.05.010

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

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

[55]. Saraswat JK, Choudhari S. Integrating big data and cloud computing into the existing system and performance impact: A case study in manufacturing. Technological Forecasting and Social Change 2025; 210:123883. https://doi.org/https://doi.org/10.1016/j.techfore.2024.123883