IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 5, Ser. II (Sep. – Oct. 2026), PP 42-51
www.iosrjournals.org

Blockchain-Based Trustless Healthcare Data Exchange in Practice with Hyperledger Fabric

Sanjeeva Polepaka[1], Balasani Venkata Ramudu[2], Rajya Lakshmi Kuruva[3], V.Rupesh[4]

[1] *Associate Professor, Department of CSE(AIML), Gokaraju Rangaraju Institute of Engineering & Technology (GRIET), Hyderabad, Telangana, India.*
[2]*Associate Professor, School of Engineering – Information Technology, Malla Reddy University, Maissammaguda, Hyderabad, Telangana, India.*
[3] *Assistant Professor, School of Engineering – CSE, Malla Reddy University, Maissammaguda, Hyderabad, Telangana, India.*
[4] *Assistant Professor, School of Engineering – Information Technology, Malla Reddy University, Maissammaguda, Hyderabad, Telangana, India.*

Abstract: *Algorithms driven by AI have been increasingly popular in the healthcare industry recently. In particular, the provision of effective patient outcomes heavily depends on access to healthcare information, including diagnostic data, patient health history, and personally identifiable information (PII). However, the need of safeguarding an individual's identity and privacy has increased as the amount of healthcare information shared between patients and healthcare providers via AI-powered systems rises. One may argue that the growing use of AI in healthcare has led to a focus on security threats and privacy and security safeguards for healthcare data, which has intensified enforcement and analysis. AI-based data protection measures are employed to address the underlying issues since these challenges are brought about by the employment of AI-based healthcare solutions to handle healthcare data. Thus, in order to preserve the privacy of healthcare data, these projects suggest AI-powered safeguards and rules. The research outlines the state-of-the-art methods for protecting patient privacy in AI-powered medical apps. Potential cyber risks, data security issues, and future directions are examined together with well-known privacy-protecting approaches like federated learning, cryptography, differential privacy methods. The project also addresses some of the pertinent data security laws and acts that control the gathering, storing, and handling of medical data in order to protect the privacy of its owners. This investigation highlights potential correction/mitigation strategies and addresses a number of gaps and uncertainties related to healthcare AI data collection processes.*

Keywords: *Healthcare Organizations (HCOs), Data Sharing, Artificial Intelligence (AI), and Data Privacy.*

Date of Submission: 14-09-2026 Date of Acceptance: 25-09-2026

I. INTRODUCTION

Artificial Intelligence, or AI, is the capacity of machines, or computers, to carry out tasks that humans do. In short, artificial intelligence is the stimulation of human-like intelligence by computer programs that mimic human behaviour artificially. However, in order for AI to function to its maximum potential, massive amounts of data and processing power are required. While processing power has likely contributed to the resurgence of AI, data has unquestionably made it possible for this technology to achieve all of its early accomplishments [1]. AI-enabled software solutions have been adopted more and more recently. In several industries, AI has remarkably become a common factor or method for processing large amounts of data, making it easier for people to make complicated decisions that are not just difficult but also impossible. This is due to the substantial volumes of the amount of data (also called big data) produced nowadays far exceeds human capacity to absorb, comprehend, and consume [2].

AI-powered solutions have been gradually used in the healthcare industry. In a survey conducted in 2021, just 25% of healthcare providers worldwide said that they have significantly incorporated AI models into their data architecture. The most popular AI-enabled solution at the time was natural language processing (NLP). During this time, the global market for healthcare AI was valued at USD 11.06 billion. The market is expected to reach over USD 188 billion in 2030, having grown to USD 20.65 billion in 2023.

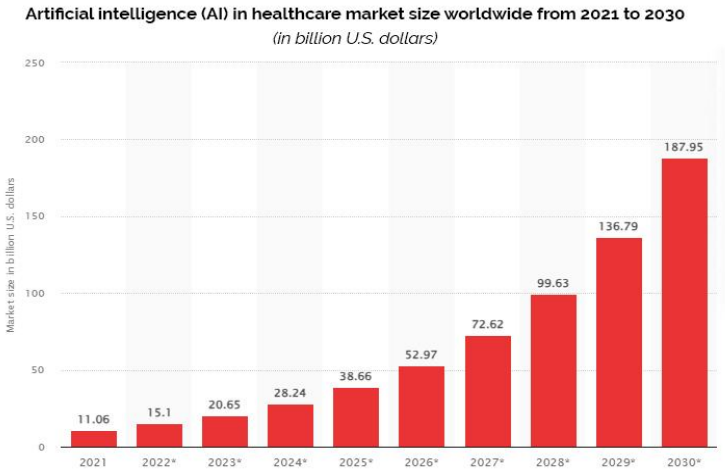

Fig 1. Healthcare AI market size globally (2021 - 2030) [3]

Artificial Intelligence (AI)-powered healthcare systems and procedures involve incorporating AI technologies and algorithms into many healthcare disciplines. Artificial intelligence (AI) is used by AI-enabled healthcare systems to analyse massive amounts of medical data, produce insightful reports, and support decision-making by stakeholders in the healthcare industry. Predictive analytics, healthcare bots, virtual assistants, medical condition diagnosis and detection, individualized treatment, and many more use cases are covered by these technologies.

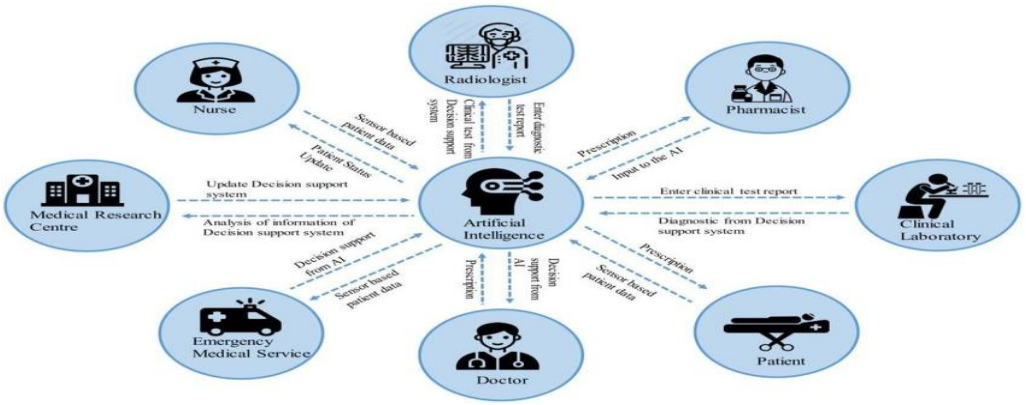

Fig 2. Applications of Healthcare AI

Machine learning (ML), deep learning (DL), computer vision, and natural language processing (NLP) are examples of AI technologies utilized in healthcare systems. The techniques cover handling, managing, analysing, and interpreting data related to healthcare, including genomes, medical imaging, sensor data, electronic health records (EHRs), and patient-generated data. In order to enhance patient care, boost productivity, and enhance health outcomes, AI-driven healthcare systems examine trends, find correlations, and learn from enormous datasets [4].

Artificial intelligence in healthcare has advanced tremendously recently, and these developments will soon have a significant impact on real-world situations. A few of the innovative AI-powered healthcare innovations are already incorporated into health systems, and more are getting close to commercialization [5]. For example, AI has shown to be especially useful in the processing of diagnostic imaging. A recent study by Stanford researchers produced an AI program that, in a matter of seconds, could identify fourteen distinct illnesses from chest X-rays [6]. AI advances have a significant impact on various healthcare areas, such as radiation oncology, organ allocation, robotics, and more [7]. But because of its explosive expansion, there is a growing public conversation concerning the advantages and risks of AI as well as how best to regulate its development [8].

Nonetheless, large volumes of training data are fundamentally needed for AI-powered healthcare approaches, therefore protecting patient data is crucial to the implementation of any AI-related research [9]. Although a centralized standard (protocol) for data encryption and sharing for AI-driven research is still lacking, the protocols are chosen on the basis of individual projects after being approved by the appropriate institutional ethics authority. For example, informed patient consent may be relinquished if an ethical commission finds that using anonymised patient diagnosis data for retrospective AI-based research is appropriate. Numerous non-proprietary, sizable healthcare data sources, like TCIA (The Cancer Imaging Archive), are likewise available to the general public and can be utilized for AI-focused research aimed at creating systematized procedures and repeatable results. Popular open-source datasets, Optimum and DDSM (Digital Database for Screening Mammography), provide carefully selected mammogram pictures that are frequently used for testing and training deep learning (DL) algorithms [10].

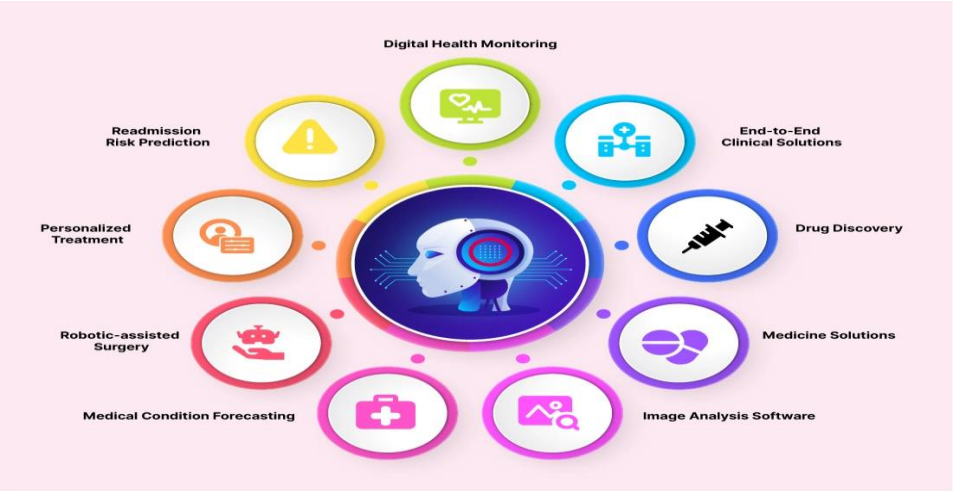

Fig 3. Healthcare application of AI and analytics

A. Importance Of Data Privacy and Security In AI-Driven Healthcare Systems:

In AI-driven healthcare systems, data security and privacy are vital because they provide the following benefits:

- Patient confidentiality: Privacy safeguards in AI-driven healthcare systems guarantee the protection of patient confidentiality. Medical records, real-time monitoring data, genetic data, and other sensitive, priceless patient information should all be handled carefully [11]. Maintaining patient privacy contributes to upholding both the patients' right to privacy and the organizations' ability to trust them.
- Information security: Healthcare systems powered by AI make extensive use of patient data. This data is vulnerable to hacking, hostile users, unhappy employees, and security breaches, manipulation, and unauthorized access [12]. To prevent unauthorized access and ensure data integrity, security solutions including firewall protection, secure storage, data encryption, and access controls are crucial.
- Informed consent: AI-powered healthcare systems typically need continuous access to patient data in order to analyse and make decisions. Obtaining consent is necessary in order to gather, keep, and use patient data in order to protect their privacy and provide them control over it [13]. Patients, as the data owners, should have control over their valuable information so they may make decisions about how to use it. This can be achieved by clear and understandable communication about how the information will be used.
- Secondary data consumption: the useful patient data acquired for artificial intelligence training has applications beyond traditional medical care. Initiatives related to public health or research may be carried out using the data. Privacy protections play a critical role in regulating the use of information for secondary purposes, guaranteeing ethical behaviour, and averting the unapproved use or disclosure of patient information.
- Reducing or moderating bias and discrimination: AI systems used in healthcare may be susceptible to bias, which could result in unfair or discriminating outcomes. In order to ensure that the training data used to train the AI models is representative, diversified, and anonymized—thus reducing biases—data privacy and security are essential. In the end, this encourages the unbiased and equitable provision of healthcare.
- Regulatory compliance: HCOs must abide by data security laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States, the General Data Protection Regulation (GDPR) of the European Union, and the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS).

Although following these data protection rules is required by law, doing so helps ensure that patient data is handled securely and in a way that respects their right to privacy [14].

o Maintains public confidence: Privacy violations and improper use of data surely reduce public faith in AI-powered healthcare solutions. The public's trust in the healthcare industry, which uses AI technologies, is increased when study data protection and privacy procedures are put in place. Building trust between patients, AI-driven healthcare technologies, and healthcare providers is greatly facilitated by transparent data processing procedures and open communication on patient privacy protection.

B. Data Protection In AI-Driven Healthcare Systems:

o AI-powered healthcare solutions cover a wide range of use cases wherein AI algorithms are applied to improve many elements of healthcare and improve patient outcomes. AI-enabled healthcare systems make use of AI's capacity to evaluate vast volumes of medical data, produce insightful findings, and support medical stakeholders in making defensible decisions [15]. The summary below explains the main components of AI-driven healthcare systems:

o Information gathering: A variety of medical data, including information from medical imaging, electronic health records (EHRs), wearable technology, sensor-derived data, genomic information, and patient-generated data, must be gathered in order to provide AI-driven healthcare solutions. Comprehensive monitoring data, medical history, and condition information about patients are all included in the different sources of healthcare data.

o Data analysis and decision-making: Healthcare data is analysed and interpreted using AI-powered algorithms, enabling improved analytics and, ultimately, well-informed decision-making. Medical professionals can utilize machine learning (ML) techniques such as supervised, unsupervised, and reinforced learning to detect patterns, identify abnormalities, predict outcomes, and provide personalized recommendations.

o Medical Diagnostics and Imaging: AI-driven healthcare solutions are having a significant influence on medical imaging analysis these days. Healthcare AI is used to analyze medical pictures, including X-rays, CT scans, and MRIs, in order to assist in the detection and diagnosis of diseases and health issues, including malignancies, neurological disorders, and cardiovascular diseases [16]. In order to improve the accuracy of disease detection, AI algorithms are also used in automated picture identification and segmentation systems.

o Personalized care and planning: Clinical guidelines, medical literature, and patient data analysis are used by AI-based algorithms to plan patient care. They offer individualized treatment plans, help with medication interactions, and information on side effects. Precision medicine, in which treatment regimens are tailored based on an individual's genetic profile using genomic data, is made possible by AI-powered healthcare systems.

o Remote patient surveillance: AI-powered healthcare technologies help doctors keep an eye on patients from a distance, giving them the ability to gather crucial data about treatment compliance and illness symptoms. Healthcare providers might be alerted to anomalies or emergencies by these technologies, which evaluate patient data in real time. For the treatment of long-term illnesses and following surgery, these solutions are especially crucial.

o Medical chatbots and virtual assistants: AI-powered chatbots and virtual assistants are indispensable in the healthcare industry. They may aid with appointment scheduling, answer queries, and give patients personalized health information [17]. Artificial intelligence (AI)-driven conversational solutions use natural language processing (NLP) to understand and respond to patient inquiries, improving access to medical records and reducing administrative work.

o Clinical and pharmaceutical research: AI-driven healthcare systems significantly speed up drug manufacture and discovery processes. In order to predict drug efficiency, find important therapeutic targets, and improve clinical trial design, artificial intelligence is utilized to evaluate enormous volumes of data. More efficient and affordable medication production is promised by this AI use case in medicine.

o Allocating resources more efficiently, improving consultation and treatment timetables, and anticipating patient flow are just a few of the ways AI-powered healthcare systems can streamline medical procedures. Healthcare providers may reduce waiting times, streamline workflows, and increase operational performance with the help of machine learning and predictive analytics techniques.

II. BACKGROUND

A. Artificial Intelligence (AI) And Data Privacy:

When implementing or developing AI-powered systems, users typically wish to safeguard sensitive, valuable data. Data privacy is therefore very important in the healthcare industry. Let's examine medical research or an AI model that was developed using electronic health records (EHRs) by healthcare specialists. Private information should be transmitted via secure medium to the computation party if the owner of the data and the computation party are not the same. But it would presumably have to be kept on the compute server and kept unaltered, meaning it shouldn't be encrypted or modified. This would make the sensitive data vulnerable to both external and internal threats, raising security risks such as theft, manipulation, or damage. As a result, there are several components to data privacy, such as characteristics, precise values, and membership of the information.

Within the context of big data and machine learning (ML), data privacy refers to safeguarding data from adversarial attacks that aim to steal important and sensitive information from a target without causing unintentional data leaks. Big data has completely changed the digital world, and its effects are becoming more and more widespread as more companies and sectors use big data analytics. In order to protect our privacy in the current digital era, it is crucial that we have control over how we share, store, and update our data. With the emergence of powerful web-enabled data mining technologies, data privacy has progressively gained social attention over time. The growth of big data has made data privacy and control over personal data increasingly crucial AI ear; The threats related to personal privacy are increased by the essential components of artificial intelligence and privacy preservation.

B. Development Of Progressive Healthcare AI:

Over the past few years, healthcare AI has grown significantly. These days, crucial medical procedures including medical imaging, drug R&D, medical bots, decision-making support, and virtual assistant activities are all handled by AI-driven solutions [18]. Over the last ten years, a number of healthcare AI-developed solutions have received approval from key authorities and regulators. Solutions for respiratory, ophthalmology, cardiology, and orthopaedics are among these technologies. Particularly, industries that create and implement best-in-class healthcare solutions, such as drug research and AI-driven medical imaging, have experienced rapid expansion.

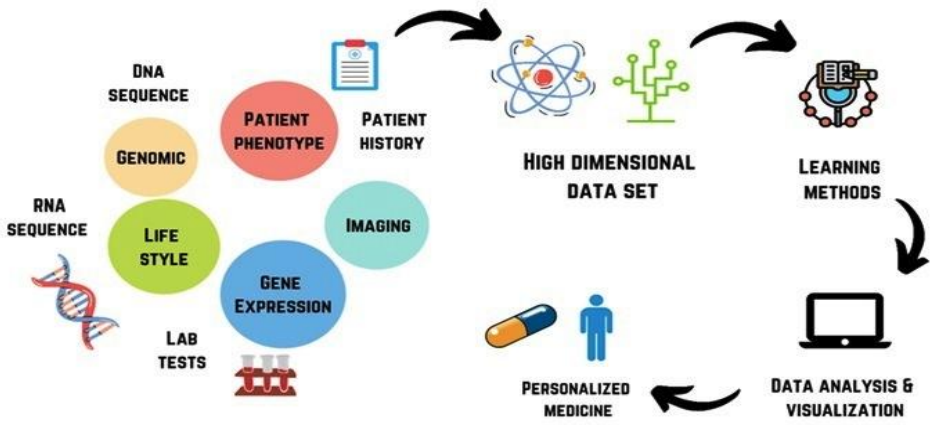

Fig 4. Training AI-algorithms used in healthcare with patient data.

AI has a "vast potential to strengthen the healthcare delivery," according to the World Health Organization (WHO) [19]. These days, artificial intelligence (AI) technologies help a number of medical endeavours, including medication discovery, imaging, disease detection, and customized treatment. Artificial intelligence supports the implementation of interventions such as infection monitoring, outbreak response, and healthcare systems management in the fields of epidemiology and public health [20]. However, there are hazards and difficulties with AI use related to human rights and healthcare ethics. AI applications, for instance, jeopardize people's privacy, affect people's autonomy and dignity in making decisions, and are linked to algorithmic biases. Large volumes of patient data are being collected and exchanged among many medical stakeholders for a variety of purposes, and digital technologies are being used more and more to record and preserve this data. Data sharing

has never been more profitable or convenient, but since healthcare AI is based on the aggregation and use of patient data, privacy protection issues have grown more complex.

However, there has never been a consistent privacy rights legislation in the past. Privacy laws and rules have typically been imprecise, disjointed, and even inadequately implemented. Data breaches in the healthcare industry have undermined public trust in data processing, and personal information has been breached on a regular basis. The sustained development of healthcare AI is typically discouraged by such instances, which are often accompanied by social political spaces where people's right to privacy is subordinated to social aims.

C. Modern Healthcare AI Protects Patient Data Privacy:

Researchers at the Technical University of Munich (TUM) have created a model technology that safeguards private patient data while educating healthcare AI systems [22]. Since then, their creation has been used in an algorithm that uses X-ray pictures to identify pneumonia in children. When it came to identifying a particular type of pneumonia in children, the scientists found that their innovative privacy protection system performed about as well as or better than conventional methods [22].

AI algorithms can be used by clinicians to diagnose illnesses and ailments such as sepsis and malignant cells, which are found in tumours. Healthcare data is typically shared throughout HCOs to maximize the pool of data, and the quantity and quality of information used for training determines how effective AI algorithms are. Scientists contend that although data protection techniques like anonymization and pseudonymization are frequently employed to safeguard and preserve data, they are insufficient. An interdisciplinary research team from the Technical University of Munich (TUM), Imperial College London in the UK, and the non-profit organization Open Mined took on this challenge and developed an innovative set of AI-driven diagnostic procedures to conduct radiological images while maintaining data privacy.

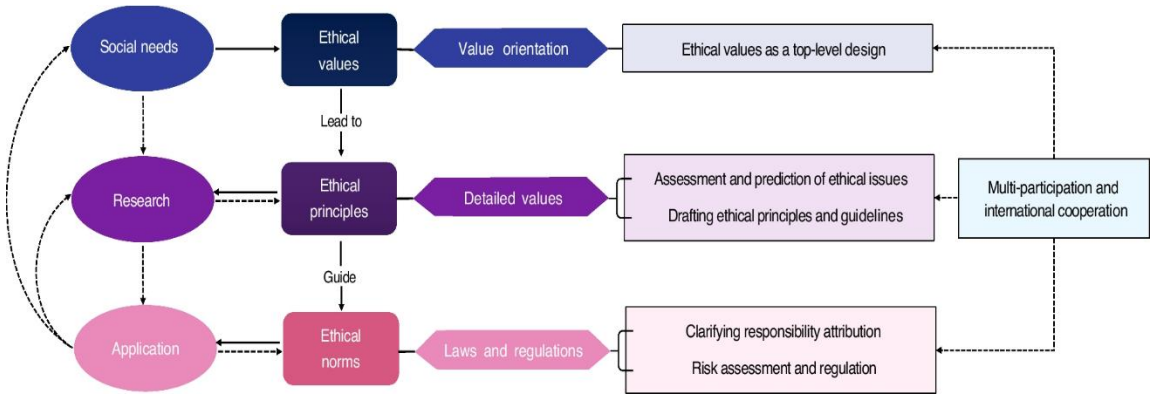

Fig 5. Ethical and Legal aspects considered in the protection of Healthcare AI application

Retaining patient data at the collecting site rather than transferring it to other HCOs is a major security measure. However, the majority of HCOs transmit duplicate databases to other HCOs that deal with AI algorithm training in order to share patient information. Additionally, the trainers use unique methods like the aggregation technique to guarantee the identification of the organization where the AI algorithms were trained in an anonymous manner [22]. In this case, the training team combines the AI algorithms in an encrypted format, which it will then decrypt following training. Additionally, to prevent the patients' private information from being filtered and revealing their names, to make sure that only statistical connections and not human contributions are taken from the data, researchers developing the AI algorithms can employ a third technique.

III. MATERIALS AND METHOD

A. Research Information:

A recent development in healthcare AI privacy security was empirically studied and presented in this qualitative evaluation. Study was done on corresponding research that was carried out by different groups and researchers. Official reports from pertinent government authorities were also examined with regard to the preservation and breach of healthcare data. In addition, news articles about the disclosure of private information were examined. Data was also gathered and analysis was done on information regarding litigation and criminal cases that were decided in court. In order to gather pertinent data about patient privacy protection worldwide, the official websites of several governments were examined. In order to compile comprehensive data on privacy

protection policies, laws, and regulations worldwide, the study accessed multiple professional legal databases using keywords such as "data privacy," "personal data," "informed consent," "Healthcare AI," "AI privacy," and "cross-border information flow," among other terms.

B. Research Methods:

A comprehensive review of the literature on the evolution of data privacy protection laws worldwide for medical data used to train artificial intelligence systems and algorithms was done. This study was grounded in an empirical analysis of laws and regulations pertaining to cross-border privacy protection, law enforcement tactics, and legal ramifications. Additionally, a study was done to find out how various regulatory bodies react to situations involving personal data.

Furthermore, a global comparative analysis of data privacy protection policies was conducted. Government sources, both official and informal, provided pertinent data privacy preservation rules from several nations. These were compiled into a rubric for thorough comparison and analysis. Further investigation into official descriptions from the respective governments and various legal sources was carried out in addition to the identification of the disparities between the laws. A comparison of the various data privacy protection legal requirements revealed weaknesses in several of the existing privacy regulations.

Fig 6. Processes and materials employed in this project

IV. RESULTS

A. Cradle, Regulatory Status and Legal Practice:

After Alan Turing released his groundbreaking study "Computing Machinery and Intelligence," which explored machine intelligence and proposed ideas like the "Turing Test," in the 1950s, the idea that sophisticated computer programs may mimic human intelligence was first put out. Backward chaining expert technology, which used MYCIN goal-directed control programs, first gained prominence in the 1970s and brought advanced healthcare AI applications into the public eye. Despite the ethical and legal concerns surrounding the use of computers in healthcare, the MYCIN system employed AI algorithms to detect infections linked to blood clotting disorders. As a result, its usage in medicine did not fully develop. Watson introduced a more sophisticated artificial intelligence (AI) system for healthcare in 2007 that employed AI to create a system for answering questions known as Deep-QA. Medical practitioners can make well-informed judgments by using the healthcare AI technology, which is currently referred to as Watson Health or just Mirative. It analyses enormous volumes of healthcare data and provides individualized, evidence-based health recommendations [23]. Additionally, additional AI-powered healthcare AI solutions, such as Google's DeepMind and Microsoft's Bio Model Analyzer, are essential for boosting patient care and clinical operations [24].

The globe has advanced significantly in the area of healthcare AI since the beginning of 2021. Additionally, during the past 20 years, the size of the healthcare AI market has grown significantly, with clinical decision support systems (CDSS) showing the highest growth rate. Healthcare data breaches are becoming more likely as a result of AI's quick development and application in healthcare technologies. For example, a significant proportion of medical imaging data that has not been sufficiently desensitized is exported because these data sets contain enormous amounts of confidential patient information. It is advised to develop reasonable and practical

data security and privacy protection policies and procedures since breaches involving private patient information may violate those patients' rights to privacy.

Regarding the legal implications and court cases, for example, the Chinese Supreme People's Court discovered in its annual work report that in 2021 the nation's courts had dealt with about 4098 lawsuits pertaining to various criminal offenses against citizens' private data, representing a 60.2% increase from the previous year. The identification cards, address books, courier lists, and WeChat accounts that were stolen and sold were all involved in the crimes [25]. In a well-known data privacy case known as "China's First Facial Recognition Case," the intermediate People's Court in Hangzhou handled important information. The ruling highlighted the necessity for healthcare providers and data handlers to conduct lawful gathering, which was crucial for the nation's regulations governing personal data and data privacy and consumption of personal information.

B. Data Privacy Protection Frameworks:

a. Acts and Policies:

o The General Data Protection Regulation (GDPR) is a data security law enacted by the European Union that went into effect in 2018. Although its standards are limited to the EU, any nation outside of Europe can utilize them as a reference. In essence, GDPR encourages the creation of digital technologies that take data owners' privacy into account.

o The Health Care Portability and Accountability Act of 1996 (HIPAA): This federal statute was first proposed in 1996. This law establishes guidelines for the handling and processing of patient health data and forbids disclosure of such information without consent or knowledge from the patient.

o The Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS): an initiative to create policies and standards for autonomous and intelligent systems with the goal of ensuring their security, moral compliance, and social benefit. In order to improve public understanding of ethical concerns related to technology, the act also places a strong emphasis on encouraging public engagement in the creation of ethical frameworks.

o The Digital Personal Data Protection Bill, 2023, was first proposed in 2019 and finally passed in 2023 after public comment. This law governs the use of all electronic personal data and stipulates that it may only be used with the owner's informed agreement. However, it also allows for certain circumstances in which the use of the data may be permitted depending on the authority and intended use. In addition, the statute requires the data's fiduciaries to maintain accuracy, safeguard it, and remove it after the intended use has been fulfilled.

o The statute, being Indian in origin, forbids the export of personal data outside of India, with the exception of those nations designated by the Indian government. According to the legislation, if someone is found guilty of violating data privacy rules or failing to set up sufficient data security measures to prevent data breaches, they will have to pay a certain amount of fine.

b. Models-Based Data Privacy Protection Methods:

The Federated Learning Technique involves conducting trials at the transferring networks rather than the data itself, as sensitive data transfers can result in data leaks and can be particularly chaotic when done across borders. Federated learning is a distributed learning strategy that combines the efforts of multiple clients to jointly create a safe model while protecting the privacy of their input [26]. The model that emerges from the training process in federated learning is trained using a variety of data sets, and learning is carried out independently each time with a new set of data.

o Cryptographic approaches: as the name implies, these techniques help data processors preserve data privacy by enabling them to encrypt data before using it for testing and training. The two main categories of cryptographic data privacy protection techniques are Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE).

o Differential privacy technique: this is a mathematical technique that attempts to conceal each participant's contribution by adding noise or randomness to valuable data.

o Hybrid privacy-preserving method: to ensure data security and privacy in the healthcare industry, this hybrid strategy includes all of the data privacy protection strategies listed above [27].

V. CONCLUSION

The use of AI technology in healthcare opens up new avenues for advancement and improves patient outcomes; however, there are a number of data security issues pertaining to patient privacy that need to be addressed, most notably the regulation of patient healthcare data handling and processing prior to, during, and

following AI algorithm training. The development of a legislative protection strategy or framework should strike a balance between data privacy protection and technical innovation. Medical attention In their quest for limitless technology to obtain a competitive edge and appease their stakeholders, service providers must to be prohibited from violating patients' rights to privacy. Additionally, as the goal of any technical improvement is to raise the standard of living for all people, technological growth and profits should not be attained at the price of other people's privacy.

Legal requirements for the handling of valuable, sensitive personal data and the implementation of data security and insider controls apply to healthcare organizations and other relevant processors of patient data. Authorities should issue special regulations in conjunction with well-known data security domain-specific laws like the Personal Information Protection Law (PIPL) to create a dual regulatory structure, that is, "basic law + special law that defines healthcare and health data processing policies," in order to build a strong legal framework to protect data privacy, which is a critical gap in many AI-specific laws. Several steps within the framework must be completed:

- Create a unified framework for health data concepts across several legal documents;
- Categorize data and develop a number of guidelines for specific data categories; and
- Improve the interactive aspect of consent through digital informed and dynamic consent to increase the effectiveness of "informed consent;" and
- Provide a strong accountability framework to ensure that the infringement of privacy rights in healthcare AI is controlled and lessened.

Moreover, nations and healthcare institutions should actively participate in creating a worldwide legislative architecture for healthcare data governance in order to expand avenues for data sharing and create a global network for information governance in the medical field. In light of the disparities and ambiguities in information governance regulations across different nations, global soft law should be used to strengthen information protection and promote cross-border information exchange. Finally, to support strong data privacy, healthcare providers should take into account the World Health Organization's (WHO) guidelines on healthcare AI governance.

REFERENCES

[1]Jumper J., Evans R., Pritzel A., Green T., Figurnov M., Ronneberger O., Tunyasuvunakool K., Bates R., Žídek A., Potapenko A., Highly accurate protein structure prediction with AlphaFold Nature, 2021 596 (7873) pp. 583-589
[2]Milana C., Ashta A. Artificial intelligence techniques in finance and financial markets: A survey of the literature. 2021. 30 (3) pp. 189-209
[3]Statista. Artificial intelligence (AI) in healthcare market size worldwide from 2021 to2030. 2024. Available at: https://www.statista.com/statistics/1334826/ai-in-healthcare-market- size-worldwide/#:~:text=It%20was%20forecast%20that%20the
[4]Vemuri, Naveen. AI-Optimized DevOps for Streamlined Cloud CI/CD. International Journal of Innovative Science and Research Technology: 2024. 9.7.10.5281/zenodo.10673085.
[5]National Intelligence Council. Global Trends 2040: A More Contested World, 2021. COSIMO REPORTS. 9781646794973, 1646794974
[6]Hutan Ashrafian, Niklas Lidströmer. Artificial Intelligence in Medicine. 2022. Springer International Publishing.
[7]Halling-Brown MD, Warren LM, Ward D, Lewis E, Mackenzie A, Wallis MG, et al. OPTIMAM Mammography Image Database: A Large-Scale Resource of Mammography Images and Clinical Data. Radiol Artif Intell. 2021; 3:e200103.
[8]Murdoch B. Privacy and artificial intelligence: Challenges for protecting health information in a new era. BMC Med Ethics. 2021; 22:122.
[9]Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated machine learning and its use in diseases prediction. Sensors (Basel) 2023; 23:2112.
[10] Sailakshmi V. Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud; 2021.
[11] Kayoe, S., & Godwin, O. Examining the effects of worldwide developments, such as the emergence of online learning and the growing emphasis on global cooperation: 2023.
[12] Nyathani, Ramesh. Integration of Industry 4.0 and Human Resources: Evolving Human Capital Management and Employee Experience through Digital Innovations: 2022.
[13] Kayoe, S., & Godwin, O. Examining the effects of worldwide developments, such as the emergence of online learning and the growing emphasis on global cooperation: 2023.
[14] Bernd Carsten Stahl. Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies. 2021. Springer International Publishing
[15] Kalla, Dinesh & Samaah, Fnu & Kuraku, Sivaraju & Smith, Nathan. Phishing Detection Implementation Using Databricks and Artificial Intelligence. SSRN Electronic Journal. 2023. 185. 10.2139/ssrn.4452780.
[16] Chowdhury D., Dey A., Garai R., Adhikary S., Dwivedi A.D., Ghosh U., Alnumay W.S. Decrypt: A 3DES inspired optimised cryptographic algorithm J. Ambient Intell. Humaniz. Comput. (2022), pp. 1-11
[17] Paul J., Annamalai M.S.M.S., Ming W., Al Badawi A., Veeravalli B., Aung K.M.M. Privacy-preserving collective learning with homomorphic encryption IEEE Access, 9 (2021), pp. 132084-132096
[18] Rasheed K., Qayyum A., Ghaly M., Al-Fuqaha A., Razi A., Qadir J. Explainable, trustworthy, and ethical machine learning for healthcare: A survey Comput. Biol. Med. (2022), Article 106043
[19] World Health Organization Ethics and Governance of Artificial Intelligence for Health. [(Accessed on 24 February 2024)]. Available online: https://www.who.int/publications/i/item/9789240029200
[20] Zeng D., Cao Z., Neill D.B. (2021). Artificial Intelligence in Medicine: Artificial intelligence–enabled public health surveillance, From local detection to global epidemic monitoring and control; Academic Press; Cambridge, MA, USA: pp. 437–453.
[21] Akgün M., Pfeifer N., Kohlbacher O. Efficient privacy-preserving whole genome variant queries Bioinformatics (2022)

[22] Caroline Brogan. New AI technology protects privacy in healthcare settings.(2021). Available at: https://www.imperial.ac.uk/news/222093/new-ai-technology-protects- privacy-healthcare/
[23] IBM. IMB Watson Health. [(Accessed on 27 February 2024)]. Available online: https://www.ibm.com/watson-health.
[24] Bass D. Microsoft Develops AI to Help Cancer Doctors Find the Right Treatments. [(Accessed on 27 February 2024)]. Available online: https://www.bloomberg.com/news/articles/2016-09-20/microsoft- develops-ai-to-help-cancer-doctors-find-the-right-treatments
[25] Work Report of the Supreme People's Court. At the Fifth Session of the Thirteenth National People's Congress on 8 March 2022. [(Accessed on 28 February 2024)]; Available online: https://www.court.gov.cn/zixun-xiangqing-349601.html
[26] Ali A., Ilahi I., Qayyum A., Mohammed I., Al-Fuqaha A., Qadir J. Incentive-driven federated learning and associated security challenges: A systematic review (2021)
[27] Torkzadehmahani R, Nasirigerdeh R, Blumenthal DB, Kacprowski T, List M, Matschinske J, Privacy-Preserving artificial intelligence techniques in Biomedicine. Methods Inf Med. (2022). 61: e12–27.