Role of AI in Healthcare. A Conceptual Study on Its Cyber Safety and Security in India

Dr. E. Nafeza[1], Ms. M.R. Iswarya[2]
[1]*Assistant Professor, Department of Business Administration (SHIFT -II), Anna Adarsh College for Women, Anna Nagar, Chennai – 600040*
[2]*Assistant Professor, Department of Business Administration (SHIFT -II), Anna Adarsh College for women, Anna Nagar, Chennai – 600040*

Abstract-The rapidly developing business environment in India is bringing many challenges and some top of the mind business issues for the Indian Sector. As organisations strive to adapt to the ever-evolving technological landscape, the intersection of artificial intelligence (AI) continues to revolutionise healthcare, it brings immense opportunities for improved patient outcomes, cost efficiency, and operational effectiveness. However, the integration of AI into healthcare systems also presents significant cybersecurity challenges. This research paper explores the intersection of AI and healthcare, focusing on the implications for cyber safety and security. By analysing current trends, challenges, and best practices, this paper aims to provide insights into effectively leveraging AI while safeguarding sensitive healthcare data from cyber threats.

Keywords: ***Indian Service Sector, Artificial Intelligence transformations, Health Care, Cyber Security***

INTRODUCTION

Healthcare systems around the world face significant challenges in achieving the 'quadruple aim' for healthcare: improve population health, improve the patient's experience of care, enhance caregiver experience and reduce the rising cost of care. Ageing populations, growing burden of chronic diseases and rising costs of healthcare globally are challenging governments, payers, regulators and providers to innovate and transform models of healthcare delivery. Moreover, against a backdrop now catalysed by the global pandemic, healthcare systems find themselves challenged to 'perform' (deliver effective, high-quality care) and 'transform' care at scale by leveraging real-world data driven insights directly into patient care. The pandemic has also highlighted the shortages in healthcare workforce and inequities in the access to care, previously articulated by The King's Fund and the World Health Organization.

By examining the intersection of AI and healthcare with a focus on cybersecurity, this research paper aims to contribute to the ongoing dialogue on effectively harnessing the potential of AI while mitigating associated risks. Through comprehensive analysis and recommendations, it endeavours to guide healthcare organisations towards secure and resilient AI implementations, ultimately ensuring the integrity, confidentiality, and availability of patient data in an increasingly digitised healthcare landscape.

LITERATURE REVIEW

Health systems worldwide are at a crossroads and face exponential healthcare cost developments that have far outpaced GDP growth rates to support health system Sustainability. This matter was very straightforward with the emergence of the 2019 coronavirus disease. (J. Pers. Med. 2023)

As health systems depend on firm disease management pathways and evidence-based care tactics to meet needs and regulate practices according to industrial healthcare delivery services, the concept of "HRO" emphasises a Highly Reliable Organization (HRO) by having its services managed by either an "accountable care organisation (ACO)" or a "health maintenance organisation (HMO)"(Shakeel, T, 2022)

The rise of biomedical science, including genomics, digital medicine, artificial intelligence (AI), and its subset, namely, machine learning (ML), provides the backdrop to healthcare transformation, with novel emerging technologies, and there is a prerequisite of a new type of labour force and standard of practice. Genomics and other technologies, including biometrics, tissue engineering, and the vaccine

industry, can improve and transform diagnostics, therapeutics, care delivery, regenerative treatment, and precision medicine models. (Khan, R.A.; Jawaid, 2022)

Scientists noted that the advancement of wearable technology and the potential of using ML and AI in healthcare is an idea that has already been explored. Thus, patient monitoring and management via virtual care with active and sensible wearable technology solutions have become a reality and part of the standards of care. In addition, AI plays a role in controlling chronic diseases such as diabetes mellitus, hypertension, sleep apnea, and chronic bronchial asthma using wearable, non-invasive sensors. (Mak, K.-K.; Pichika, 2019)

AI comprises the application of artificial neural networks, i.e., deep learning techniques named Generative Adversarial Networks (GANs), that impact the field of radiology. GANs contain two artificial neural networks, i.e., (i) a generator that synthesises images similar to real images, and (ii) a discriminator that reveals the difference between synthetic and real images.(Carroll, W.M.2019)

OBJECTIVES OF THE STUDY

- To examine the theoretical underpinnings of AI in Healthcare, with reference to its Cyber Safety and Security.
- To elucidate the role of AI in Healthcare.
- To analyse the impact of AI in Healthcare, and its integration in Indian sectors.
- To identify challenges and opportunities associated with this integration.

ROLE OF AI IN HEALTHCARE

Healthcare is one of the major success stories of our times. Medical science has improved rapidly, raising life expectancy around the world, but as longevity increases, healthcare systems face growing demand for their services, rising costs and a workforce that is struggling to meet the needs of its patients.

Demand is driven by a combination of unstoppable forces: population ageing, changing patient expectations, a shift in lifestyle choices, and the never-ending cycle of innovation being but a few. Of these, the implications from an ageing population stand out. By 2050, one in four people in Europe and North America will be over the age of 65 this means the health systems will have to deal with more patients with complex needs. Managing such patients is expensive and requires systems to shift from an episodic care-based philosophy to one that is much more proactive and focused on long-term care management.

Healthcare spending is simply not keeping up. Without major structural and transformational change, healthcare systems will struggle to remain sustainable. Health systems also need a larger workforce, but although the global economy could create 40 million new health-sector jobs by 2030, there is still a projected shortfall of 9.9 million physicians, nurses and midwives globally over the same period, according to the World Health Organization.1 We need not only to attract, train and retain more healthcare professionals, but we also need to ensure their time is used where it adds most value—caring for patients.

Building on automation, artificial intelligence (AI) has the potential to revolutionise healthcare and help address some of the challenges set out above. There are several definitions of AI, but this report draws from a concise and helpful definition used by the European Parliament, “AI is the capability of a computer program to perform tasks or reasoning processes that we usually associate with intelligence in a human being.”2 AI can lead to better care outcomes and improve the productivity and efficiency of care delivery. It can also improve the day-to-day life of healthcare practitioners, letting them spend more time looking after patients and in so doing, raise staff morale and improve retention. It can even get life-saving treatments to market faster. At the same time, questions have been raised about the impact AI could have on patients, practitioners, and health systems, and about its potential risks; there are ethical debates around how AI and the data that underpins it should be used.

IMPACT OF AI IN HEALTHCARE, AND ITS INTEGRATION IN INDIAN SECTORS

AI is now top-of-mind for healthcare decision makers, governments, investors and innovators, and the European Union itself. An increasing number of governments have set out aspirations for AI in healthcare, in countries as diverse as Finland,

Germany, the United Kingdom, Israel, China, and the United States and many are investing heavily in AI-related research.

Three phases of scaling AI in healthcare: First, solutions are likely to address the low-hanging fruit of routine, repetitive and largely administrative tasks, which absorb significant time of doctors and nurses, optimising healthcare operations and increasing adoption. In this first phase, we would also include AI applications based on imaging, which are already in use in specialties such as radiology, pathology, and ophthalmology.

In the second phase, we expect more AI solutions that support the shift from hospital-based to home-based care, such as remote monitoring, AI-powered alerting systems, or virtual assistants, as patients take increasing ownership of their care. This phase could also include a broader use of NLP solutions in the hospital and home setting, and more use of AI in a broader number of specialties, such as oncology, cardiology, or neurology, where advances are already being made. This will require AI to be embedded more extensively in clinical workflows, through the intensive engagement of professional bodies and providers. It will also require well designed and integrated solutions to use existing technologies effectively in new contexts. This scaling up of AI deployment would be fuelled by a combination of technological advancements (e.g., in deep learning, NLP, connectivity etc.) and cultural change and capability building within organisations.

In the third phase, we would expect to see more AI solutions in clinical practice based on evidence from clinical trials, with increasing focus on improved and scaled clinical decision-support (CDS) tools in a sector that has learned lessons from earlier attempts to introduce such tools into clinical practice and has adapted its mind-set, culture and skills. Ultimately respondents would expect to see AI as an integral part of the healthcare value chain, from how we learn, to how we investigate and deliver care, to how we improve the health of populations. Important preconditions for AI to deliver its full potential in European healthcare will be the integration of broader data sets across organisations, strong governance to continuously improve data quality, and greater confidence from organisations, practitioners and patients in both the AI solutions and the ability to manage the related risks.

CHALLENGES OF AI IN HEALTHCARE

The inherent challenges of machine learning, the imperfection of ethics and laws, and the poor acceptance by society have all hindered the development of AI.

Ethical issues:

- Data ethics: Data ethics is the foundation of AI, and its key areas include informed consent, privacy and data protection, ownership, objectivity, and transparency. This "guardianship" reflects the reality that there are interests in patients' medical records, and these interests are protected by law.
- Ethics of clinical practice: The introduction of AI to healthcare practice brings new challenges to doctors. Although a strictly rule-oriented robot may initially seem more reliable, an ethical person is more trustworthy in situations where complex clinical practice decisions are required. AI tends to amplify biassed findings regardless of the specific clinical interactions.

Legal issues arising in AI:

- Healthcare workers undergo strict assessments before they are employed, and they should abide by a series of codes of conduct in daily practice. No globally unified laws or regulations regarding the application of AI in medicine are currently in place to standardise the behaviour of practitioners. If AI is used by criminals, AI-crime (a new and destructive crime) may occur.
- Therefore, the formulation of broad and detailed AI laws is urgently needed. However, several issues must be considered. Finally, we must continuously upgrade the laws that have been formulated. Studies have shown that health-related data have far exceeded the original expectations of the original privacy protection laws (such as the HIPAA Act of the US Congress in 1996).37–39 Fortunately, many new laws have been introduced to regulate AI data protection, responsibility determination, and supervision.

Security:

- Hardware security: All AI products currently require a series of electronic products to perform their functions, such as computers, mobile

phones, and bracelets. Three key issues regarding the security of such hardware must be noted.

- Software security: Even algorithm programs with powerful functions are very vulnerable under design attacks.47–50 The performance of the AI system is often unsatisfactory in a targeted design confrontation despite its performance being excellent in the initial design inspection. In fact, all stages of the AI algorithm formation process will be attacked, assuming that the attacker knows everything related to the trained neural network model (training data, model architecture, hyperparameters, number of layers, activation function, and model weights)
- Human factors: Today's AI is realised by software codes. When dealing with thousands of codes, engineers will inevitably make mistakes. An AI system can be improved through subsequent patches and updates. However, in the AI programs used in the medical field, such errors may directly endanger the health of patients.

OPPORTUNITIES OF AI IN HEALTHCARE

The intersection of artificial intelligence (AI) and healthcare offers numerous opportunities for improving patient outcomes, optimising healthcare delivery, and enhancing cyber safety and security. Here are some key areas where AI can be applied in healthcare with a focus on cyber safety and security:

- Predictive Analytics for Cyber Threat Detection: AI algorithms can analyse vast amounts of healthcare data to identify patterns indicative of cyber threats such as malware, ransomware, and unauthorised access attempts. Predictive analytics can help healthcare organisations anticipate and mitigate potential cybersecurity breaches before they occur.
- Behavioral Analytics for Anomaly Detection: AI-powered behavioural analytics can monitor user activity within healthcare systems to detect anomalous behaviour that may indicate a cybersecurity breach. By establishing baseline behaviour for users and systems, AI algorithms can identify deviations that could signal a security threat.
- Secure Data Sharing and Interoperability: AI technologies can facilitate secure data sharing and interoperability among healthcare providers, enabling seamless exchange of patient information while maintaining privacy and security. Techniques such as federated learning allow multiple parties to collaborate on AI model development without sharing sensitive patient data directly.
- Privacy-Preserving AI Techniques: Privacy-preserving AI techniques such as homomorphic encryption, differential privacy, and secure multiparty computation enable analysis of sensitive healthcare data while protecting patient privacy. These techniques allow healthcare organisations to derive insights from data without exposing it to unauthorised access.
- Medical Device Security: AI can enhance the security of medical devices by identifying vulnerabilities, detecting abnormal device behaviour, and implementing proactive security measures. AI algorithms can continuously monitor medical devices for signs of compromise or unauthorised access, helping to prevent potential cyberattacks on critical healthcare infrastructure.
- Regulatory Compliance and Risk Management: AI can assist healthcare organisations in achieving regulatory compliance with cybersecurity standards such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). AI-powered risk assessment tools can identify and prioritise cybersecurity risks, enabling organisations to allocate resources effectively to mitigate threats.

CONCLUSION

In summary, AI presents significant opportunities for improving cybersecurity in healthcare by enabling proactive threat detection, enhancing data privacy, securing medical devices, ensuring regulatory compliance, and promoting cybersecurity awareness among healthcare professionals. By leveraging AI technologies effectively, healthcare organisations can strengthen their cybersecurity posture and better protect patient information from evolving cyber threats

REFERENCE

[1] J.Pers.Med.2023,13,951.https://doi.org/10.3390/jpm13060951 https://www.mdpi.com/journal/jpm

J. Pers. Med. 2023,13, 951 2 of 22(COVID-19) pandemic and the Ukraine war.

[2] Shakeel, T.; Habib, S.; Boulila, W.; Koubaa, A.; Javed, A.R.; Rizwan, M.; Gadekallu, T.R.; Sufiyan, M. A survey on COVID-19 impact in the healthcare domain: Worldwide market implementation, applications, security and privacy issues, challenges and future prospects. Complex Intell. Syst. 2022,9, 1027–1058.

[3] Khan, R.A.; Jawaid, M.; Khan, A.R.; Sajjad, M. ChatGPT-Reshaping medical education and clinical management. Pak. J. Med. Sci. 2023,39, 7653.

[4] Mak, K.-K.; Pichika, M.R. Artificial intelligence in drug development: Present status and future prospects. Drug Discov. Today 2019,24, 773–780.

[5] Carroll, W.M. Digital health and new technologies. In Nursing and Informatics for the 21st Century Embracing a Digital World,3rd ed.; Productivity Press: New York, NY, USA, 2022;

[6] Confederation of Indian Industry. (2015). Eastern India: A potential IoT hub. Retrieved fromhttp://cii.in/PublicationDetail. Ministry of Micro, Small & Medium Enterprises. Retrieved from http://www.dcmsme.gov.in/MSE-CDProg.htm (last accessed on 17 February 2017)