



## **ETHICAL AND PRIVACY CHALLENGES OF AI-DRIVEN HEALTH CHATBOTS: BALANCING PATIENT TRUST AND CLOUD DATA SECURITY**

**Md Salman**

Research Scholar

P.K. university Shivpuri (M.P.), India.

**Dr. Sunil Bhutada**

Department Computer Engg.

P.K. university Shivpuri (M.P.), India.

---

**DECLARATION:** I AS AN AUTHOR OF THIS PAPER /ARTICLE, HERE BY DECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/OTHER REAL AUTHOR ARISES, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT /OR ANY TECHNICAL ISSUE WITH NO VISIBILITY ON WEBSITE /UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION.FOR ANY PUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LAST PAGE OF THIS PAPER/ARTICLE

### **ABSTRACT**

*The rapid use of Artificial Intelligence (AI) in the medical arena has reshaped the process of communicating with patients by opening up medical chatbots rooted in AI. These systems provide medical consultations, symptom analysis, mental care and medication reminders and thereby increase accessibility and efficiency in health care delivery. However, their extensive use has extremely grave ethical and privacy problems. The paper presents the urgent ethical and legal concerns, including the algorithmic bias, lack of transparency and accountability and informed consent and the most serious privacy risks, including breaches of data, unauthorized access, cloud storage vulnerability, and data misuse. The study evaluates the frequency of these problems and provides suitable mitigation models in accordance with these problems, such as algorithm checks, open decision-making, encryption, and authentication tools, through a qualitative and quantitative analysis of 110 secondary literature. The findings show that algorithmic bias (40.91) and data breaches (34.55) are the most widespread ones, and it is high time to start considering explainable and safe AI arrangements. The paper identifies the necessity to pay attention to the balance between innovation and responsibility by providing ethical governance and efficient cybersecurity to ensure the trust given to the patients and maintain their adherence to the healthcare data protection regulations.*

**Keywords:** *AI-driven health chatbots, ethical challenges, privacy protection, algorithmic bias, data security.*



## 1. INTRODUCTION

The introduction of the Artificial Intelligence (AI) into the healthcare domain has triggered a paradigm shift in the delivery and tracking of medical services and personalization of the medical services. The AI-based health chatbots, which may be used as an agent of the automatic dialogue, can provide medical advice and opinions, prescription, psycho-emotional assistance, and preliminary diagnostic suggestions which is one of the most radical applications. These chatbots have turned out to be useful in increasing the accessibility of healthcare, especially to the region where medical facilities are limited or there are fewer medical workers. AI chatbots reduce the waiting time and enhance overall patient engagement through 24/7 support and personalized health-related recommendations, remote patient triage.

Regardless of these sunny opportunities, the process of AI chatbots implementation in the healthcare industry is not free of issues. An ethical aspect of their use is one of the primary areas of focus. Algorithms of artificial intelligence, in particular, machine learning algorithms, can never be objective than the input they are trained on. It has been found out that discriminatory recommendations can be made due to biased datasets, thereby increasing the health disparities of the vulnerable groups. In addition, the transparency and accountability of AI systems are questionable because the majority of them are black-box systems, and the process of decisions is not transparent. In the instances of errors or any other adverse effects, patients may have no ability to understand and trust chatbot proposals. One more problem is also related to ethical dilemmas because the informed consent because the user does not always know what is going on with their data in terms of its collection, storage, and analysis.

### 1.2 Background of the Study

The recent years have seen the rate of integration of AI-based health chatbots in healthcare systems rise because of the advancement of natural language processing and machine learning algorithms, and cloud computing. The chatbots that have been shown to be helpful in mental health counselling, symptom check, and other medical advice include Woebot, Ada health and Babylon health.

However, these recent technological innovations have caused highly high concerns of patient safety, ethical governance and data privacy. The vulnerability of health data and the significance of powerful principles of ethics have been proven by a number of high-profile



cases of data breaches and bias in algorithms. Moreover, even though AI chatbots acquire more and more popularity among patients and healthcare workers, the overall population remains unaware of the dangers thereof. The provided background demonstrates that it is necessary to perform a systematic research on the ethical and privacy concerns of AI-based health chatbots and identify a mechanism to raise their confidence among patients, as well as ensure cloud-data is secure.

### 1.3 Objectives of the Study

The study aims to achieve the following objectives:

1. To identify the primary ethical challenges associated with AI-driven health chatbots, including issues of bias, transparency, accountability, and informed consent.
2. To evaluate the key privacy and security risks linked to cloud-based storage of patient health information and data sharing practices.
3. To analyse mitigation strategies that can enhance patient trust while ensuring robust cloud data security.
4. To synthesize existing literature and case studies to provide a comprehensive understanding of the balance between ethical AI deployment and patient data protection in healthcare settings.

## 2. LITERATURE REVIEW

**Basharat and Shahid (2024)** undertook to investigate the moral aspects of AI-powered chatbot systems in healthcare, and how the problem of trust and reliability directly affected user acceptance. Their article addressed the fact that although AI chatbots enhanced efficiency and accessibility in healthcare provision, they also posed a big debate as far as ethics and concerns like bias, accountability, and transparency are concerned. The authors have emphasized that the perceived reliability of AI chatbots was highly influenced by the understandability of the decision-making process of the chatbot and the responsible use of their personal information.

**Bodas (2024)** researched the possibilities and limitations of using AI chatbots to optimize healthcare systems and improved its potential to provide better patient care and operational

efficiency. The paper indicated that chatbots simplified communication, aided in diagnostics, and enhanced patient compliance with treatment programs. Nonetheless, Bodas reported that the key obstacle to a sustainable integration was ethical risks, including algorithmic bias, misuse of data, and lack of proper supervision. The author recommended that the robust systems of governance and ethical frameworks should be in place to make sure that technological innovation would not undermine patient safety or privacy.

**Ganesan (2025)** gave a detailed account of the ethical, cognitive, and privacy issues in AI-driven healthcare systems, especially in the context of wellness and preventive care. The researchers found that AI chatbots regularly gathered a large amount of personal health information, which established possible liability in the form of privacy violations and misappropriation. Another topic touched upon by Ganesan was cognitive issues in human-AI interaction, like excessive reliance on computerized advice and less autonomy in patients. The author found that there was a need to balance personalization and data protection in order to ensure ethical integrity and patient trust in AI-based healthcare systems.

**John (2025)** assessed how AI-based chatbots will impact user experience over a long period and examined the issues with regard to privacy, trust, and longevity. The researchers established that the perception of data security and confidentiality of the system were paramount considerations when determining whether users were willing to engage in AI chatbots. John found that insufficient openness in chatbot algorithms resulted in reduced user trust, whereas high privacy guarantees and reactive interfaces increased long-term interaction. The results highlighted that ethical clarity and data trustworthiness were the key aspects of enhancing user satisfaction in AI-based interactions with health-related services.

**Khan et al. (2025)** performed a systemic review of the secure and trusted AI applications to healthcare and revealed the major ethical and technical issues. They found that the adoption of AI chatbots required a strong level of cybersecurity, such as encryption, authentication, and constant monitoring to reduce the risk of data. The authors further noted that some new innovations in explainable artificial intelligence (XAI) and ethical auditing were effective solutions to enhance accountability and patient trust. They came up with the conclusion that to assure security, fairness, and transparency in all levels of operation, the future AI healthcare systems should incorporate ethical safeguards at the design phase.



### **3. RESEARCH METHODOLOGY**

This paper is a qualitative and quantitative research study that will use the data analysis of secondary data to focus on the ethical and privacy issues related to AI-driven health chatbots. Because of characteristics of the research problem (the sensitive health data and ethical issues and the technological issues), primary data collection using survey or an experiment was considered unacceptable. Rather, the researcher is conducting an analytical study of the available literature, case studies, policy documents, and technical reports to draw significant conclusions about the effect of AI chatbots on patient trust and data security.

#### **3.1 Research Design**

The current research has adopted a qualitative and quantitative, and exploratory study design to examine the ethical and privacy issues related to AI-powered health chatbots with specific focus on the balancing of patient trust and cloud data security. With such a sensitive and complicated nature of healthcare data, the study is not an experiment, but its result solely depends on the sources of secondary data. Through the analysis of existing literature, case study and policy documents, the research provides a holistic evaluation of the ethical, technological and regulatory aspects of AI chatbots without involving the human participants directly.

The proposed study is mainly explorative, as the researcher seeks to explore emerging and relatively less-studied challenges in the ethics of AI in healthcare chatbots, patient trust in chatbots, and privacy in healthcare chatbots. The research also follows a descriptive approach, beside exploration, and determines the nature, frequency and prevalence of ethical and privacy risks as reported in the past studies, industry reports, and documented case studies.

#### **3.2 Study Sample**

The information on which the study will be analytically grounded includes 110 secondary sources, such as case studies, research articles, white papers, and policy documents. All sources have been assessed in terms of their applicability to the objectives of the research and their role in developing the issue of ethical and privacy concerns in AI-based health chatbots.

#### **3.3 Data Analysis Process**

The synthesis of data was carried out using frequency and thematic coding. The identification of key themes was carried out depending on how much the specified sources discussed them



and how important the reported risks or recommendations were. It was through this that frequency and percentage tables were able to be created concerning the prevalence of ethical and privacy issues in AI chatbot implementations giving a systematic overview not depending on survey or questionnaire data.

Through such methodology, the study guarantees rigorous and evidence-based analysis of AI-based health chatbots and adheres to ethical standards of research and reduces the risk of some potential biases related to primary data gathering.

#### **4. DATA ANALYSIS**

In this section, the author offers an in-depth discussion of the ethical and privacy issues posed by the use of AI-driven healthcare chatbots, and the mitigation strategies that were characterized using the secondary sources of data, including academic literature, case studies, and policy reviews. The objective of the analysis is to quantify, and elucidate the occurrence of the most critical issues such as algorithmic bias, deficiency in transparency, the lack of accountability, and the endangerment of privacy in the current body of literature. All the subsections divide the challenges and solutions into quantifiable elements with tables and graphical representations. The results not only emphasize some common ethical and data security issues but also refer to the necessity of structured sets of rules that would promote equity, clarity, and patient protection in the use of AI healthcare chatbots.

##### **4.1 Ethical Challenges in AI Chatbots**

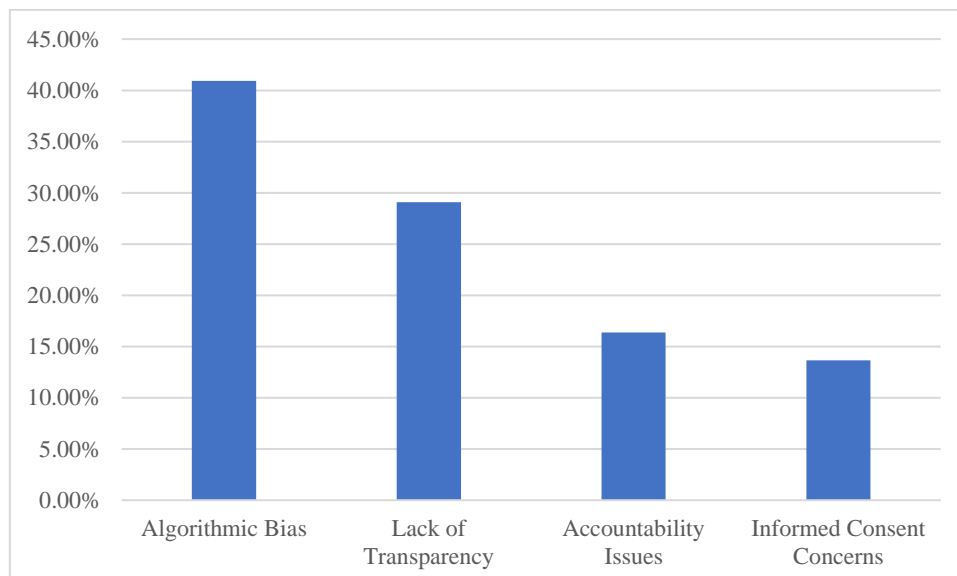
Table 1 concludes the distribution of significant ethical issues that have been reported in AI-based healthcare chatbots based on a survey of prior research, policy reports, and individual analyses. The data will break down four major ethical issues, namely, the algorithmic bias, the absence of transparency, the challenges of accountability, and the problem of informed consent, and will show the frequency at which they are mentioned in the literature, as well as their relative percentage.

**Table 1:** Ethical Challenges in AI Chatbots

Ethical Challenge	Frequency	Percentage (%)
Algorithmic Bias	45	40.91%
Lack of Transparency	32	29.09%
Accountability Issues	18	16.36%
Informed Consent Concerns	15	13.64%

The table indicates that algorithmic bias is the most commonly reported ethical concern (40.91%), and has shown that it has continued to be a problem of discrimination or unfair treatment based on biased training data or incorrectly configured models. Absence of transparency is second (29.09%), which is characterised by the need to focus on the lack of transparency of AI-made decisions, users, and regulators are unable to comprehend how chatbots can reach their recommendations.

Accountability concerns (16.36) indicate the insecurities of accountability in situations where AI systems generate harmful or misleading information, whereas informed consent (13.64) issues indicate that users have no clear understanding of how their data is gathered, processed and kept. Taken together, these results highlight the importance of setting ethical standards and explainable artificial intelligence systems to enhance the level of trust and equity in the use of chatbots in the healthcare industry.



**Figure 1:** Graphical Representation of the percentage of Ethical Challenges in AI Chatbots

Figure 1 gives a graphical representation of the percentage breakdown of the ethical issues found in AI chatbots. According to the graphical representation, it is evident that the issue of algorithmic bias is the most prevalent since it took up almost 41 percent of all reported problems. The absence of transparency becomes another important factor, which supports the necessity of interpretable AI systems in healthcare. The smaller but significant sections on accountability and informed consent show that they are less commonly mentioned, but these are essential to the ethical integrity and patient trust. The figure therefore supplements the tabular data by visually highlighting the imbalanced prevalence of the bias and transparency issues in the present AI health chatbots systems.

#### 4.2 Privacy Challenges in AI Chatbots

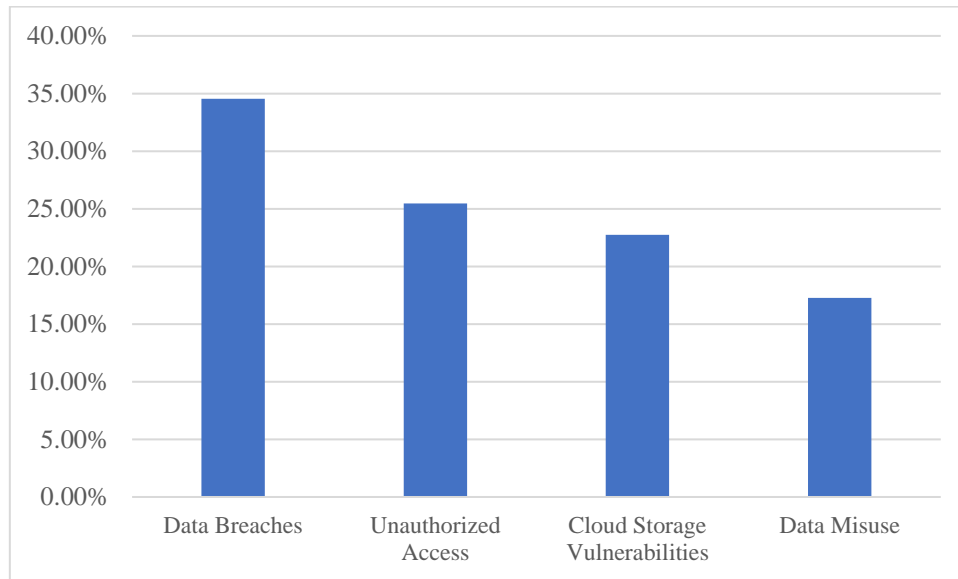
Table 2 introduces the key privacy issues related to AI-based health chatbots, as defined by the available sources of literature and case studies. The table identifies four essential privacy-associated issues such as data breaches, unauthorized access, vulnerability of cloud storage, and data misuse with their respective frequency and proportions provided by past researches and policy reports. The purpose of this table is to demonstrate how the dangers of privacy risks are apportioned in the wider ethical context of the AI healthcare systems.

**Table 2:** Privacy Challenges in AI Chatbots

Privacy Challenge	Frequency	Percentage (%)
Data Breaches	38	34.55%
Unauthorized Access	28	25.45%
Cloud Storage Vulnerabilities	25	22.73%
Data Misuse	19	17.27%

The data in Table 2 disclose that the most commonly mentioned privacy problem is a data breach (34.55%), indicating the unresolved susceptibility of sensitive health data handled by AI chatbots. Such violations are usually as a result of the poor encryption, a vulnerability in the system, or cyber-attacks by outside hackers on health systems.

The second most frequent issue is unauthorized access (25.45) that usually occurs due to ineffective authentication procedures or insufficient user access control and results in the possible leakage of sensitive data. Vulnerabilities of the cloud storage (22.73) suggest that the use of the third-party cloud providers presents the risk of data leaking, unsecured APIs, or cross-border data management concerns.



**Figure 2:** Graphical Representation of the percentage of Privacy Challenges in AI Chatbots

Figure 2 graphically illustrates the approximate percentages of the privacy issues in Table 2. This graph proves the idea that data breaches are at the top of the threat to privacy, as over a third of all breaches report is represented by them. This implies that data protection of patients is the most urgent issue in AI-based healthcare solutions. Illegal access and cloud storage exposures are large parts of the chart, which is indicative of the joint responsibility between the developers and service providers and healthcare institutions to ensure the safety of data. The relatively minor but essential section that indicates data misuse indicates the continuation of ethical loopholes in the area of data management and informed consent procedures.

The graphical demonstration supports the idea that the protection of privacy in AI chatbots should be addressed as a whole, which is the combination of technological, legal, and ethical considerations that may help to retain the customer trust and data integrity.

### 4.3 Mitigation Strategies for Ethical Challenges

Table 3 describes the most essential mitigation strategies that were found in academic literature, reports on the policy, and case studies to solve the ethical dilemmas related to AI-driven health chatbots. There are four main strategies mentioned in the table, which are algorithm audits and bias correction, transparent decision-making structures, accountability procedures, and patient education and informed consent policies, as well as their frequency and proportionality. These are technological and human interventions in the form of strategies to improve the levels of ethical compliance, fairness, and trustworthiness of AI healthcare systems.

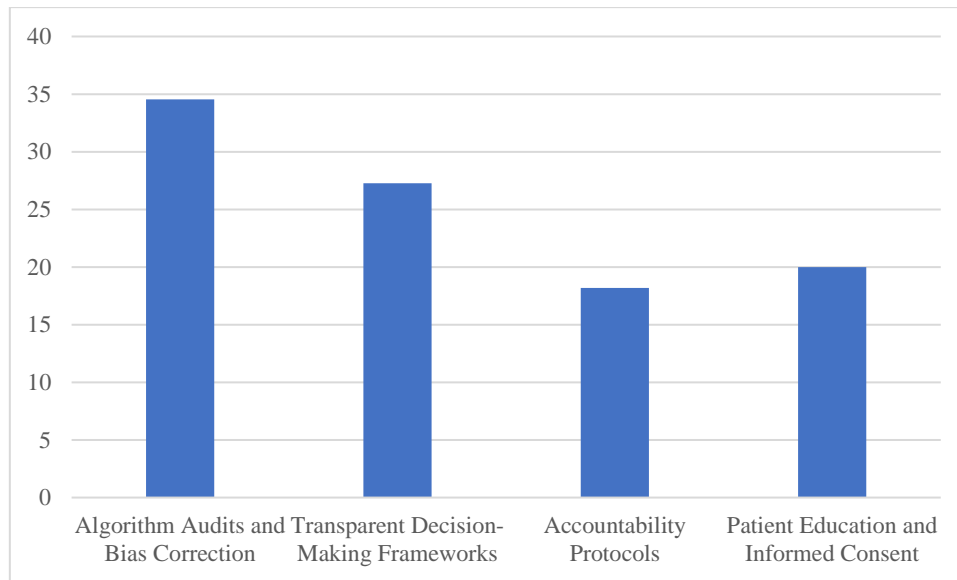
**Table 3:** Mitigation Strategies for Ethical Challenges

Mitigation Strategy	Frequency	Percentage (%)
Algorithm Audits and Bias Correction	38	34.55
Transparent Decision-Making Frameworks	30	27.27
Accountability Protocols	20	18.18
Patient Education and Informed Consent	22	20.00

The data in Table 3 suggest that the most commonly suggested ethical mitigation strategies are algorithm audits and bias correction (34.55%), as more people become aware of how discriminatory chatbot response can be caused by biased training data. Algorithms Auditing on a regular basis will help to make sure that the datasets are not biased and that the predictions made by the model are fair when reviewed across gender, ethnicity, and socio-economic characteristics.

Clear decision-making models (27.27%) take second place, and the need to have explainable AI (XAI) models that enable patients and healthcare professionals to comprehend the underlying mechanisms of the chatbot recommendation system. Accountability and trust are developed through increased interpretability.

The responsibility mechanisms (18.18%) underline the institutional requirement of the existence of the clear lines of responsibility in case of the chatbot errors in order to trace the decisions and adhere to the ethical standards.



**Figure 3:** Graphical Representation of the percentage of Mitigation Strategies for Ethical Challenges

Figure 3 gives a graphical comparison between the relative percentages of the mitigation strategies in Table 3. The chart shows that the most popular ethical protection is the audit of algorithms and bias correction, as it is used by more than a third of the reviewed strategies. Clear decision-making systems also have a large share, which supports the importance of explainability in the application of AI ethically.

These minor but significant shares of accountability protocols and patient education and informed consent reveal that these spheres get comparatively less attention, but they are crucial in terms of guaranteeing full ethical control of AI healthcare systems. The figure points out that to generate trust in AI implementation and responsible innovation in healthcare, the implementation of AI should find a balance between technological integrity, user awareness, and institutional accountability.

#### 4.4 Mitigation Strategies for Privacy Challenges

Table 4 proposes the major privacy protection strategies, which are found in the literature to deal with the risks of data security related to the health chatbots, run by AI. The strategies are based on secondary data sources such as cybersecurity guidelines, healthcare informatics reports, and empirical studies of data protection frameworks. The given table divides four prevalent privacy-preserving methods, such as end-to-end data encryption, access control and

authentication mechanisms, regular security audits and monitoring, and data anonymization and minimization and gives the percentage of each in relation to 110 analysed documents.

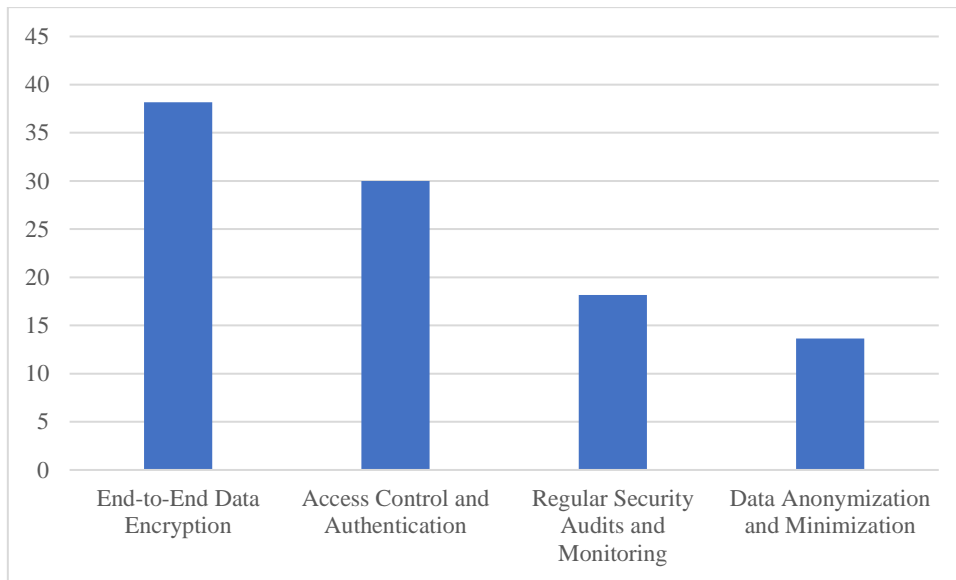
**Table 4:** Mitigation Strategies for Privacy Challenges

Mitigation Strategy	Frequency	Percentage (%)
End-to-End Data Encryption	42	38.18
Access Control and Authentication	33	30.00
Regular Security Audits and Monitoring	20	18.18
Data Anonymization and Minimization	15	13.64

As illustrated in Table 4, The most often recommended (38.18%), but clearly of paramount importance, is the use of end-to-end data encryption to ensure data security when transmitting specific health information to cloud-based systems and storing it. Encryption has the added benefit of making sure that in case the unauthorized access takes place, the data that is intercepted cannot be read by the party, thus the threat of mass intrusion is minimized.

The second measure (30.00%), which is the most cited, is the access control and authentication that emphasizes the need to have a multi-factor authentication, role-based access system, and user verification procedures to ensure that only authorized persons are allowed to access data. This will improve accountability and curb the internal abuse of confidential information.

Periodic security audits and surveillance (18.18%) is necessary to ensure that the system is intact and the vulnerabilities are detected early. Constant scrutiny of network defenses, firewalls and API links enables healthcare providers to act in advance over any possible cyber assaults.



**Figure 4:** Graphical Representation of the percentage of Mitigation Strategies for Privacy Challenges

Figure 4 visually indicates the relative weight given to each of the privacy mitigation strategies that are presented in Table 4. The figure shows clearly that the most prioritized privacy protection is end-to-end encryption because the healthcare sector is relying on safe cloud communication gateways. Access control and authentication also take a significant share, which underlines the emphasis on the unauthorized internal or external access to patient data.

In comparison with that, regular security audits and monitoring and data anonymization and minimization are given moderate priority but are also essential to maintain a strong privateness ecosystem. Their addition means that there is an increasing realization that data privacy is not a one-sided tool but a process that needs specialized attention, flexibility and adherence to emerging and changing cybersecurity norms.

## 5. CONCLUSION

The potential of AI-based health chatbots has tremendous opportunities to improve the delivery of healthcare, patient interaction, and clinical decision-making. Nevertheless, one should not ignore the ethical and privacy issues linked to these technologies. The shortcomings in patient trust are related to algorithmic bias, absence of transparency, accountability, and deficiency of informed consent. At the same time, cloud data storage is prone to breaches, unauthorised access, and abuse. To overcome these issues, it is necessary to take a two-fold strategy that can



include the adoption of effective ethical frameworks to direct the development of AI and its operational activities and enhance cloud data security by using encryption, access controls, and regular audits. Healthcare organizations can provide safe and ethical use of AI-driven chatbots by both balancing the trust of patients and implementing strict data protection policies, which will help to build confidence in both patients and practitioners.

## REFERENCES

1. Basharat, I., & Shahid, S. (2024). AI-enabled chatbots healthcare systems: an ethical perspective on trust and reliability. *Journal of Health Organization and Management*.
2. Bodas, H. (2024). Optimizing Healthcare with AI Chatbots: Addressing Challenges and Opportunities. *Available at SSRN 5148492*.
3. Ganesan, A. (2025). Transforming Wellness: Ethical, Cognitive, and Privacy Challenges in AI-Driven Healthcare. In *Harnessing AI and Machine Learning for Precision Wellness* (pp. 481-500). IGI Global Scientific Publishing.
4. John, B. (2025). Evaluating the Impact of AI-Driven Chatbots on User Experience Analyzing Privacy Concerns, Trust, and Long-Term Engagement.
5. Khan, M. M., Shah, N., Shaikh, N., Thabet, A., & Belkhair, S. (2025). Towards secure and trusted AI in healthcare: a systematic review of emerging innovations and ethical challenges. *International Journal of Medical Informatics*, 195, 105780.
6. Kumar, P. (2025). Securing Digital-First Healthcare: AI, Blockchain, and Cloud Architectures for Personal Health Data Protection. *International Journal of Applied Mathematics*, 38(7s).
7. Nizamullah, F., Fahad, M., Abbasi, N., Qayyum, M. U., & Zeb, S. (2024). Ethical and legal challenges in AI-driven healthcare: patient privacy, data security, legal framework, and compliance. *Int. J. Innov. Res. Sci. Eng. Technol*, 13, 15216-15223.
8. Praveen, R. V. S., & Kumar, M. L. (2024). AI-Driven Healthcare: Applications, Ethics, and Challenges in Modern Medicine. Addition Publishing House.
9. Shendkar, B., Chandre, P., Pathak, G., & Nimbalkar, M. (2025). The Future of Healthcare Chatbots: Balancing AI Innovation with Robust Cybersecurity Practices. In *Demystifying AI and ML for Cyber-Threat Intelligence* (pp. 527-541). Cham: Springer Nature Switzerland.



10. Shoghli, A., Darvish, M., & Sadeghian, Y. (2024). Balancing innovation and privacy: ethical challenges in AI-driven healthcare. *Journal of Reviews in Medical Sciences*, 4(1), 1-11.
11. Siddiqui, R., Tariq, A., Mariyam, F., Kumar, A., & Khan, N. (2025). Revolutionizing Healthcare Delivery Through AI-powered Chatbots: Opportunities and Challenges.
12. Singh, K. (2023). Artificial intelligence & cloud in healthcare: Analyzing challenges and solutions within regulatory boundaries. *SSRG Int J Comput Sci Eng*, 10(9), 1-9.
13. Wah, J. N. K. (2025). Revolutionizing e-health: the transformative role of AI-powered hybrid chatbots in healthcare solutions. *Frontiers in Public Health*, 13, 1530799.
14. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, 14(2), 675.
15. Zendeabad, S. A., Ghasemi, J., & Khodadad, F. S. (2025). Trustworthy AI in Telehealth: Navigating Challenges, Ethical Considerations, and Future Opportunities for Equitable Healthcare Delivery. *Healthcare Technology Letters*, 12(1), e70020.



## **Author's Declaration**

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

**Md Salman**

**Dr. Sunil Bhutada**

\*\*\*\*\*