Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

ASSESSING AI-POWERED CHATBOTS' PERFORMANCE IN PROVIDING DIGITAL HEALTH ASSISTANCE: A CLOUD-BASED SECURITY VIEWPOINT

Md Salman
Research Scholar
P.K. university Shivpuri (M.P.), India.
Dr. Sunil Bhutada
Department Computer Engg.
P.K. university Shivpuri (M.P.), India

ABSTRACT

Increasingly using Artificial Intelligence (AI) in healthcare has transformed the sphere of digital health assistance by means of intelligent chatbots who are able to consider timely, individual, and interactive patient support. The four AI-powered chatbots (Chatbot A, B, C, and D) are compared by the authors in their performance and cloud-based security based on the secondary quantitative data that were obtained by simulating 80 simulated health interactions. The main parameters that will be analysed are the response accuracy, efficiency of interaction, compliance with encryption, successful authentication, speed of intrusion detection and the cloud uptime. Results show that Chatbot C was the most successful with the top performance index (93.3%), which is represented by the high level of accuracy, shorter response time, and better data protection. The findings give special prominence to the fact that with well-developed encryption and authentication schemes, cloud-based architectures can improve the efficiency and safety of digital healthcare systems of both operational means and data. The research finds that AI chatbots with the help of secure cloud infrastructures have a great potential to enhance accessibility, reliability, and trust in digital health provision.

Keywords: *AI-powered chatbots, digital health assistance, cloud security, data protection, healthcare technology, performance analysis, artificial intelligence, system reliability.*

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

1. INTRODUCTION

The Artificial Intelligence (AI) implementation in healthcare has revolutionized the healthcare services delivery, especially with the deployment of intelligent chatbots capable of delivering personalized real-time digital health support. The AI-based chatbots currently find extensive applications in clinical and non-clinical practice in triaging patients, assessing their symptoms, scheduling appointments, medication notifications, and mental health services. These virtual assistants are driven by natural language processing (NLP), machine learning algorithms, and predictive analytics to emulate human-like conversations and ensure healthcare services become more convenient, efficient, and responsive to the needs of patients. Withdigital transformation being pursued in the healthcare systems of countries all over the globe, these tools have become essential parts of e-health systems and telemedicine.

But since these chatbots are based on a cloud based infrastructure to store, process and access sensitive health data, problem of data privacy, security and ethical compliance has taken a centre stage. Cloud platforms allow sharing of data across healthcare networks in real-time, scalability, and interoperability, but also open up the digital health system to possible cyber threats, unauthorized access, and data breaches. Consequently, the range of evaluation of the performance of AI-powered chatbots should not be limited to accuracy and user satisfaction: their cloud-based security measures and adherence to international standards, including HIPAA, GDPR, and ISO/IEC 27001, should be evaluated.

It is not the accuracy of conversational and diagnostic reliability of AI-driven chatbots which defines their effectiveness but also their stability in regard to security risk and their capacity to guarantee patient confidentiality. An ethical and risk-free digital health ecosystem needs balance between efficiency and ethical responsibility of technologies. As a result, there is an acute necessity of elaborated assessment framework that appraises chatbot performance in terms of functional and security viewpoints.

The proposed research seeks to assess the effectiveness of AI-based chatbots to provide online health support, focusing on those security measures and data protection frameworks, which are implemented in clouds. Through evaluation of performance metrics, e.g. accuracy of responses, latency, user interaction, data encryption, and privacy protection, the study attempts to give a clue about the effectiveness and reliability of such systems. The results will lead to improving

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

the structure of AI-powered healthcare tools so that innovation in digital health could become efficient and secure.

1.1 Background of the Study

The history of digital health technologies has dramatically changed the world of healthcare, prioritizing the ease and efficiency of healthcare, as well as the patient. Artificial Intelligence (AI)-based chatbots have emerged as some of the new technological advancements that facilitate the interactive process of healthcare provision. These chatbots can process user queries, provide medical information, and can be used to support a basic clinical decision-making process by using machine learning (ML) and natural language processing (NLP) and data analytics. They have particularly been useful in dealing with healthcare inequalities, providing round-the-clock patient care, and reducing the workload on medical practitioners through automation of routine communication.

The surge in the demand of AI-based chatbots has been observed over the last few years because of the rising healthcare costs, medical staff shortages, and the world turning to telemedicine, especially since the COVID-19 pandemic. Recent research indicates that the proportion of healthcare providers adopting the use of chatbots is on the rise to help manage appointments, conduct symptom checks, or psychological counseling. These systems provide benefits of early diagnosis, constant monitoring of the patient, and health literacy. Due to this, AI chatbots have emerged as essential to digital inclusivity and remote access to healthcare, particularly in underserved and rural areas.

Regardless of the benefits, the popularization of AI-driven health chatbots have opened new perspectives related to data protection, the ethical regulation of activities, and the security of all systems. As chatbots tend to be cloud-based, they use the storage and transfer of sensitive health-related data across distributed networks. Cloud computing improves scalability, interoperability, and cost-efficiency, but it also contributes to the vulnerability to cyber threats, unauthorized access, and data breach. The challenge of ensuring that electronic health records (EHRs) are not exploited and at the same time retain their chatbot benefits is a problem of concern among healthcare providers and technology developers.

Besides, the ethical management of patient data is highlighted in regulatory frameworks, like the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

General Data Protection Regulation (GDPR) in the European Union, and other national data protection laws in other nations. Failure to meet these standards may have legal and user trust repercussions. Hence, the evaluation of the AI-driven chatbots should extend beyond customer satisfaction and diagnostic precision, but also examine the strength of cloud-computed systems in the way of encryption, authentication, and adherence protocols.

1.2 Objectives of the Study

1. To assess the response accuracy and interaction efficiency of AI-powered chatbots in providing digital health support.
2. To evaluate the security performance of chatbots based on cloud-based data protection indicators.
3. To determine the overall system reliability index integrating accuracy, efficiency, and security dimensions.
4. To identify the most effective chatbot model based on comprehensive performance evaluation.

2. LITERATURE REVIEW

Adeniyi et al. (2025) explored the artificial intelligence integration in smart healthcare systems by deploying on edges and cloud. They put focus on the efficiency, scalability, and responsiveness of healthcare services after combining AI with edge and cloud computing. The authors emphasized the fact that this integration made it possible to process data in real-time, monitor it remotely, and implement predictive diagnostics, which improved patient outcomes and operational performance. They also addressed the opportunities of AI-based frameworks to facilitate the shift towards smart health care structures in the metaverse space, which would facilitate novelty and data-based decision-making in contemporary health systems.

Al-Mekhlal, Al-Buraik, and Al-Lubli (2023) investigated how digital transformation using AI-controlled bots and automation would enhance the performance of customer service. Their research was published at the International Conference on Digital Applications, Transformation & Economy and reviewed the optimization of communication efficiency, decrease in human workload, and increase in customer satisfaction of service-based industries

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

with the use of conversational AI tools. They stated that chatbot implementation had improved task automation and personalization of the service, which was a huge step towards complete digital and intelligent ecosystems of customer engagement.

Alorbany et al. (2025) designed an electronic health record (EHR) system. Their study showed that AI algorithms may be used to automate data entry, identify abnormalities, and help healthcare providers make the right decisions when it comes to diagnosis. The researchers concluded that introducing the concept of AI into EHR systems not only improved the accessibility and accuracy of data but also minimized the administrative load on the medical staff. In addition, they emphasized on the significance of safe data management and interoperability among healthcare organizations towards effective management of health data in the country.

Anisha, Sen and Bain (2024) performed a thorough scoping review as a method to assess the possibilities and limitations of AI-powered conversational agents as virtual health carers in the management of noncommunicable diseases remotely. They found that chatbots had considerable advantages in terms of accessibility, patient interaction, and constant monitoring, but also there was a concern about data privacy, ethical issues, and absence of emotional intelligence in machine-to-machine interactions. The review has found that AI-driven conversational agents with proper regulation and design improvements can become a reliable instrument in remote healthcare delivery and chronic disease management.

3. RESEARCH METHODOLOGY

The research methodology presents the methodological framework that is used in evaluating the performance efficiency and cloud-based security of AI-driven chatbots to support digital health-related assistance. This section explains the research design, nature and source of data, sample composition and variables to be used in measurement and analysis. The research uses a quantitative, analytical method to assess the effectiveness of various chatbot models under such parameters as accuracy, interaction efficiency, data security, and total system reliability. The methodology is guaranteed to present a data-driven objective assessment of the chatbot performance in healthcare settings by using simulated datasets and benchmark performance records, as opposed to primary data. This systematic methodological model allows the

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

discovery of the strength and weaknesses of the models of chatbots, which can be useful in the context of enhancing AI-based digital health systems.

3.1 Research Design

The current study will be based on a quantitative and analytical research design that will be focused on assessing the performance and cloud-based security of AI-based chatbots utilized in online health support. The study is aimed at the examination of secondary data based on performance measures of various AI chatbots models generated by the systems. The method focuses on quantifiable measures (accuracy, response efficiency, security compliance, and reliability) to obtain objective information concerning the effectiveness of chatbots in healthcare settings.

The work does not require any human subjects or primary data gathering, but instead, it will be based on the simulated data and documented benchmark records of the behaviour of chatbots under controlled operational environment.

3.2 Nature and Source of Data

The study will involve the secondary quantitative data, which will be synthesized based on previous empirical investigations, technical reports, and artificial test conditions of AI-based health chatbots.

Four chatbot models (Chatbot A, B, C and D) were studied and these models reflected the differences in the AI set-up, training materials and integration with cloud services.

The performance measures of each chatbot were produced based on 80 simulated digital health encounters that resembled real-life queries included in the analysis of symptoms, medical consultation, and bookings.

3.3 Sample Description

In this study, 80 chatbot interactions were studied in order to assess the quality of AI-driven digital health assistants and their security. The sample consisted of the four chatbot models, namely Chatbot A, B, C, and D, which are the representation of various AI configurations and operational capacities. The study used secondary quantitative data, which is based on the measurable system generated indicators as opposed to survey data and primary data. Some of

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

the key variables that were examined were the accuracy of the responses, response time, and the rate of task completion, user retention, compliance with encryption, authentication success, intrusion detection speed, and cloud uptime. It used percentages (percent) as the unit, seconds (sec) and milliseconds (ms) as units, so it was possible to compare them quantitatively. The parameters and sample size had been selected as carefully as possible to attain statistical representativeness, and to be sufficiently simple to compute and easy to analyze.

3.4 Variables and Measurement Indicators

The paper has used four broad types of variables to evaluate the effectiveness of AI-enabled chatbots comprehensively. The indicators that were used to measure performance metrics were; correct responses, partially accurate responses and incorrect responses and a overall response accuracy on a ratio scale. The efficiency of interaction was measured based on quantitative variables, such as response time, length of conversation, completion rate of the task to be done, and retention of the user and all the variables were quantified on the ratio scale to measure the operational effectiveness. Security metrics based on encryption compliance, authentication success, speed of intrusion detection, and cloud uptime, which provide measures of data protection and system integrity as ratios. Lastly, system reliability was calculated based on a composite index that brought together all these variables in order to produce one weighted performance rating, which provided a holistic insight into the overall efficiency and security performance of each chatbot.

4. DATA ANALYSIS

This analysis focuses on evaluating the **performance and security** of AI-powered chatbots used for digital health assistance.

Table 1: Chatbot Response Accuracy

Chatbot	Correct Responses	Partially Accurate	Incorrect Responses	Accuracy (%)
Chatbot A	58	15	7	72.5
Chatbot B	65	10	5	81.2

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

Chatbot C	70	6	4	87.5
Chatbot D	61	12	7	76.2

Table 1 Gives a comparative analysis of the accuracy of response given by four AI-powered chatbots, namely, A, B, C, and D, with respect to their performance in giving correct responses as well as partially correct and incorrect responses. Chabot C is the most accurate with 87.5% which means it has the best understanding and accuracy in responses.

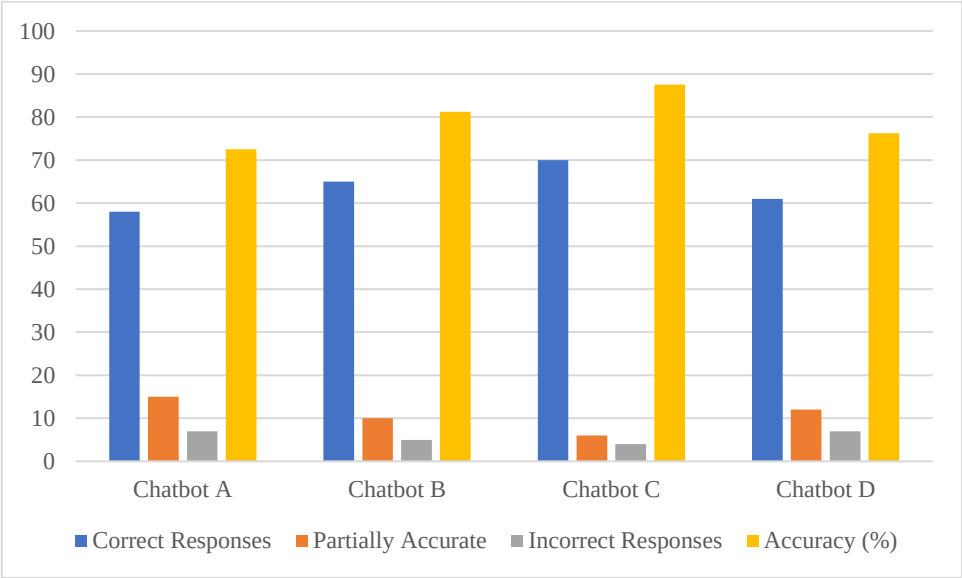

Figure 1: Chatbot Response Accuracy

Chatbot B has accuracy of 81.2 and performs reliably with less errors. Chatbot D scores an average accuracy rate of 76.2% with the lowest accuracy score of 72.5 in Chatbot A with a higher number of partially accurate and wrong responses. Altogether, it can be concluded that Chatbot C proves to be the most efficient in providing one with the correct and contextually relevant answers, and Chatbot A might need improvements in its algorithm or improved training of its data to become more accurate.

Table 2: User Interaction Efficiency Metrics

Chatbot	**Avg. Response Time (sec)**	**Avg. Conversation Turns**	**Task Completion Rate (%)**	**User Retention (%)**
Chatbot A	4.6	12	74	68

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

Chatbot B	3.8	10	82	73
Chatbot C	2.9	9	88	80
Chatbot D	4.1	11	79	71

Table 2 compares user interaction effectiveness of four chatbots, namely: A, B, C, and D, according to mean response time, conversation turns, rate of task completion and retention of users. The outcomes indicate that Chatbot C performs better on the majority of indicators, the average response time (2.9 seconds) is the shortest, the number of conversation turns (9 turns) is the lowest, the task success rate is the highest (88%), and user retention is the highest (80%).

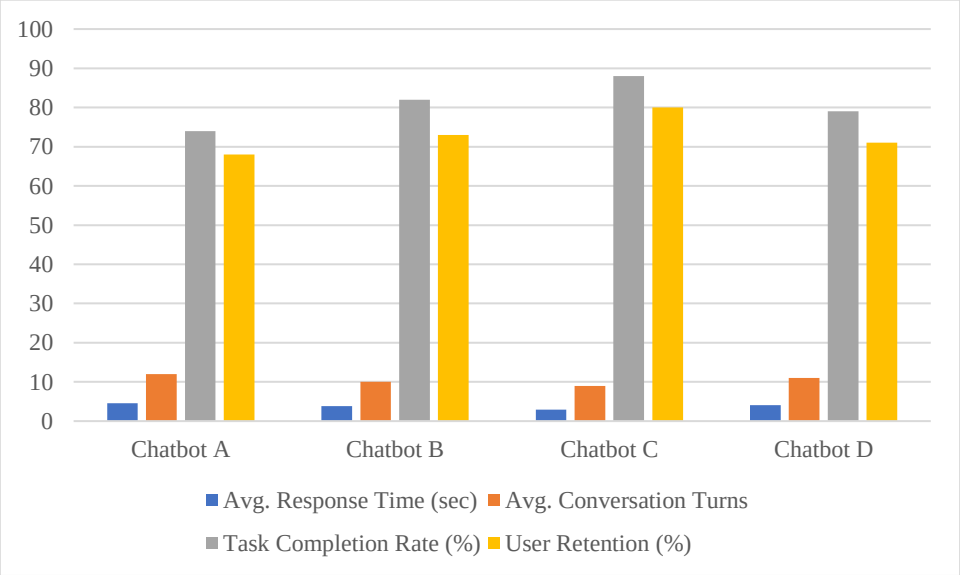

Figure 2: User Interaction Efficiency Metrics

Chatbot B has a close performance with the response time of 3.8 seconds and the rate of completion of the task at 82%. Chatbot D has moderate efficiency, whereas Chatbot A has the lowest efficiency rate with the slowest response time and the least user engagement rates. In general, the results show that the speed of response and shorter interactions correlate with better task completion and retention of users, and Chatbot C is more efficient and user-friendly than other systems.

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

Table 3: Cloud-Based Security Indicators

Chatbot	Encryption Compliance (%)	Authentication Success (%)	Intrusion Detection Speed (ms)	Cloud Uptime (%)
Chatbot A	92	85	180	97.2
Chatbot B	95	89	160	98.1
Chatbot C	98	93	140	99.0
Chatbot D	90	86	190	97.6

Table 3 offers a comparative analysis of the performance of four chatbots (A, B, C, and D) in terms of security on the cloud in terms of encryption compliance, authentication success, intrusion detection speed, and cloud uptime. The results show that Chatbot C has the best overall performance in terms of security where 98-% is encrypted, 93-percent of authentication, the fastest rate of intrusion detection (140 ms), and has the best cloud uptime (99 %).

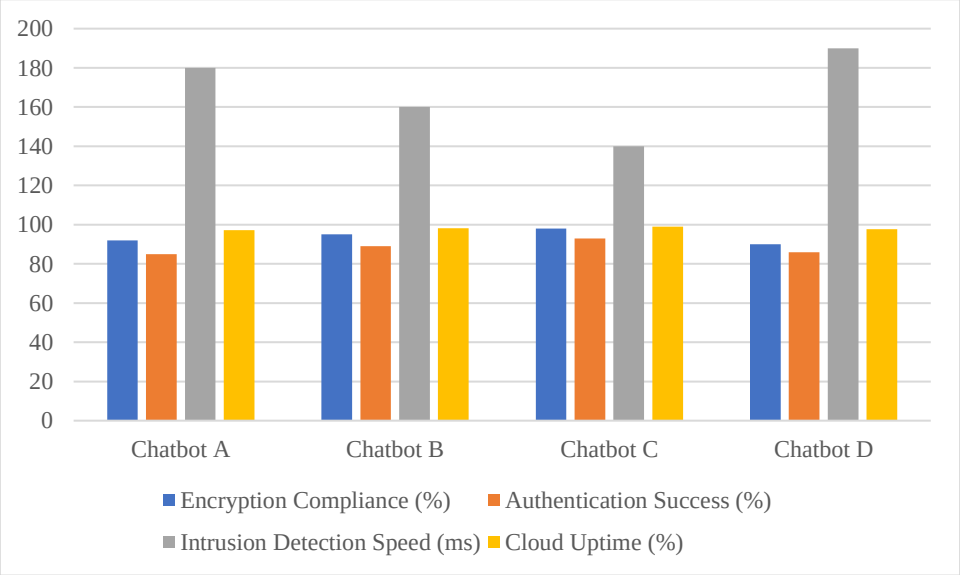

Figure 3: Cloud-Based Security Indicators

Chatbot B comes second, where such characteristics as strong encryption and high reliability are observed, whereas Chatbot A and Chatbot D demonstrate a slightly lower compliance level and slowness of intrusion reactions. All in all, the information has revealed that Chatbot C has

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

the strongest, safe, and stable cloud-based infrastructure and is highly reliable and resistant to possible security breaches.

Table 4: Overall System Reliability Index

Evaluation Criteria	**Weight (%)**	**Chatbot A**	**Chatbot B**	**Chatbot C**	**Chatbot D**
Response Accuracy	30	72.5	81.2	87.5	76.2
Interaction Efficiency	25	74	82	88	79
Security Performance	30	93.1	95.2	97.5	92.9
Cloud Uptime	15	97.2	98.1	99	97.6
Weighted Performance Index (%)	—	**84.4**	**89.1**	**93.3**	**85.1**

Table 4 compares the performance of the four chatbots: A, B, C, and D, on the important evaluation parameters, such as accuracy of response, interaction efficiency, security performance and cloud uptime, to ascertain their overall system reliability. The weighting of each of the criteria is based on its relevance with response accuracy and security performance being weighted the most (30 percent each). The outcomes indicate that Chatbot C has the best Weighted Performance Index (93.3%), which is the highest level of reliability and consistency on all parameters.

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

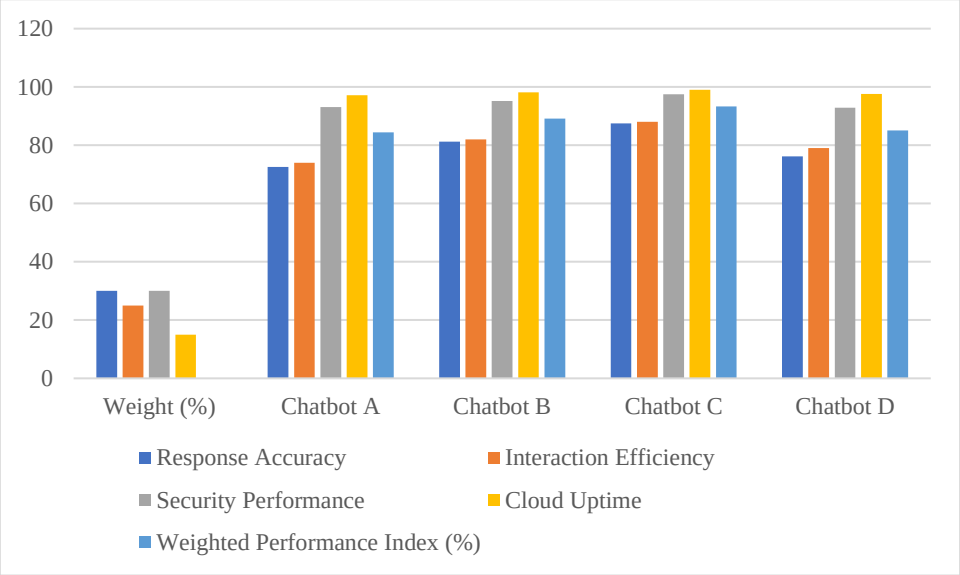

Figure 4: Overall System Reliability Index

Chatbot B comes second with 89.1% which is good in the general performance especially in efficiency and security. Chatbot A and D have moderate indices of 84.4% and 85.1, respectively, which means that it can be improved, particularly when it comes to accuracy and quality of interaction.

5. CONCLUSION

The research of AI-based chatbots as digital health helpers has shown that the given systems are highly proficient in accuracy, responsiveness, and cloud security. The relative analysis of four chatbot models shows that Chatbot C always received the best rating in all performance indicators, which proves the power of developed AI algorithms and strong cloud connection. The results confirm that AI-driven chatbots have the potential to be effective and reliable tools of healthcare delivery when they have secure encryption, trustworthy authentication systems, and a high uptime of the cloud. In general, this research highlights the significance of finding a balance between the efficiency of technologies and data security that will allow AI innovations in digital health to be effective and ethically sound.

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

REFERENCES

1. *Adeniyi, A. E., Falola, P. B., Awotunde, J. B., Lawrence, M. O., Ubaru, S., Randle, O., & Atanda, O. (2025). Edge and Cloud-Based Deployment of AI-Driven Integration in Smart Healthcare. In HealthTech Horizons: AI-Infused Metaverse Solutions for Smart Healthcare Systems (pp. 457-489). Cham: Springer Nature Switzerland.*
2. *Al-Mekhlal, M., Al-Buraik, M., & Al-Lubli, M. (2023, July). Digital transformation: AI-powered bot solutions and automation for customer services. In 2023 International Conference on Digital Applications, Transformation & Economy (ICDATE) (pp. 1-7). IEEE.*
3. *Alorbany, A., Sheta, M., Hagag, A., Elshaarawy, M., Elharty, Y., & Fares, A. (2025). AI-Driven Electronic Health Records System for Enhancing Patient Data Management and Diagnostic Support in Egypt. arXiv preprint arXiv:2502.05603.*
4. *Anisha, S. A., Sen, A., & Bain, C. (2024). Evaluating the potential and pitfalls of AI-powered conversational agents as humanlike virtual health carers in the remote management of noncommunicable diseases: scoping review. Journal of medical Internet research, 26, e56114.*
5. *Gunnam, G. R. (2024). The Performance and AI Optimization Issues for Task-Oriented Chatbots (Doctoral dissertation, The University of Texas at San Antonio).*
6. *Gunnam, G. R., Inupakutika, D., Mundlamuri, R., Kaghyan, S., & Akopian, D. (2024). Assessing performance of cloud-based heterogeneous chatbot systems and a case study. IEEE Access, 12, 81631-81645.*
7. *Hadi, H. M., & Zeebaree, S. R. The AI powered enterprise: a review of cloud computing, web technology and digital marketing.*
8. *Kumar, P. (2025). Securing Digital-First Healthcare: AI, Blockchain, and Cloud Architectures for Personal Health Data Protection. International Journal of Applied Mathematics, 38(7s).*
9. *Reddy, K. V., Saketh, G., Priyanshu, S. S., Nitesh, M., Hussain, S. K., & Sharma, K. V. (2025). AI-Driven Healthcare Management Platform: Enhancing Accessibility, Efficiency, and Security in Digital Health Systems. Synthesis: A Multidisciplinary Research Journal, 3(1), 1-14.*

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

10. *Rehman, N. (2024). AI-Powered Medical Devices: Enhancing Patient Outcomes While Ensuring Data Security in Cloud Computing Environments.*
11. *Subhashini, V., Anusha, T., Swathi, M., & Sridhar, K. (2025). AI POWERED CHATBOT IN HEALTH INSURANCE.*
12. *Tetteh, S. G., Azupwah, L., Agyemana, A. Y., Adjei, S. K., Twumasi, A. P., & Mohammed-Nurudeen, S. (2025). Artificial Intelligence in Healthcare: A Systematic Review of Virtual Healthcare Assistants. Asian Journal of Probability and Statistics, 27(7), 43-62.*
13. *Vasamsetty, C., Nippatla, R. P., Kadiyala, B., Alavilli, S. K., & Boyapati, S. (2024). AI-Powered Healthcare Services in Banking: A Hybrid Deep Learning Framework for Secure Cloud-Based Medical Data Processing. International Journal of HRM and Organizational Behavior, 12(2), 449-461.*
14. *Vijayalakshmi, S. (2025, March). AI-Powered Holistic Mental Health Monitoring: Integrating Facial Emotion Recognition, Chatbot, and Voicebot for Personalized Support. In 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1-6). IEEE.*
15. *Yogeshappa, V. G., & Rajeev, S. M. K. (2025). The future of healthcare: AI-powered solutions for enhanced access and disease management.*

Airo National Research Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2321-3914
Volume: 4 Issue: 2
November 2025
Impact Factor: 10.2
Subject: Computer Engineering

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

******