Understanding Privacy and Security Postures of Healthcare Chatbots

Aishwarya Surani
University of Denver
InSPIRIT Lab
Denver, CO, USA
aishwaryaumesh.surani@du.edu

Sanchari Das
University of Denver
InSPIRIT Lab
Denver, CO, USA
Sanchari.Das@du.edu

ABSTRACT

Chatbots are artificial communication systems used popularly for online assistance for everyday usages such as shopping, banking, food services, healthcare, and many other sectors. During the pandemic, chatbots are being extensively used in healthcare to obtain information about suitable physicians, available slots, clinics, and pharmacy working days to schedule patient appointments. Such increased chatbot usage brings additional security risks and privacy challenges that should be addressed, yet understudied. To understand these challenges, we conducted a systematic literature review starting with $1,836$ papers and doing a detailed analysis of 40 papers from diverse disciplines that examine the security and privacy of chatbots. Our findings highlight that the current research focuses on providing technological solutions that can secure user data. We conclude by identifying research gaps and providing potential solutions to enable robust data security for sensitive healthcare data accessed by healthcare chatbots.

Author Keywords

Chatbots, Healthcare, Privacy, Security, Survey, Systematic Literature Review.

CCS Concepts

•Security and privacy → Web application security; Privacy protections; •Social and professional topics → Patient privacy; Health information exchanges; Remote medicine; Personal health records; Medical records;

INTRODUCTION

Chatbots are conversational agents that interact with websites, web services, and web apps through user commands. Abdul-Kader and Woods (2015) define a chatbot as "a computer program that can hold a conversation with a human using Natural Language Speech," and "it is a computer program that mimics intelligent conversation" [1]. Chatbots are created to have a human-aligned conversation about reducing traffic to the human agents in several sectors [32]. Chatbots are designed to understand user queries and generate responses in a conversation. They can identify and consider the emotional aspects of users [16]. There has been a growing demand for using chatbots in all the sectors like education, e-commerce, banking, and healthcare [3]

Due to COVID-19, Chatbots have been used increasingly in helping patients with their queries. Laranjo et al. created a chatbot in COVID-19, *Chasey* to help track the number of people who contracted the COVID-19 virus, answer FAQs, and so on [12]. Bharti et al. created Medbot using artificial intelligence to help patients by providing healthcare suggestions, therapy sessions, and so on [5]. Chatbots provide healthcare information to patients based on their needs, help with medical treatment, and provide healthcare-related suggestions [2]. To benefit from the existing health chatbots, users need to register and provide some personal information, including some sensitive healthcare information [47]. However, the increasing demand for chatbots leads to growing security and privacy concerns. Users are unaware of how the chatbots use or share the data, which increases the privacy risk as the data is highly confidential.

To understand this further, the goal of this study is to analyze the security and privacy aspects related to chatbots. We conducted a systematic literature review to provide a broad view of the problem statement. This study highlights the current research related to the security and privacy of data in chatbots and also provides ways that can be used to protect the privacy of user data [16].

RELATED WORK

Chatbots can assist in human-computer interaction and influence the behavior of users by asking questions and responding to the users' questions [33]. In addition to speech ability, emotional intelligence is necessary for chatbots to function as a digital companions. Nowadays, chatbots are considered helpful and save much time for patients as they assist whenever needed. A good chatbot must be able to identify and consider the emotional aspects of users and function in a way that is similar to the support provided by healthcare professionals [47].

Chatbots have been extensively used in health-related applications for providing health education and diagnostics in recent

CHI'22, April 30–May 06, 2022, New Orleans, LA, USA

ISBN 978-1-4503-6708-0/20/04. . . $15.00
DOI: https://doi.org/10.1145/3313831.XXXXXXX

years; for example, chatbots can be used to get health reports. Chatbots are helpful as they provide fast responses to users' queries and are also available. They are also used to predict particular diseases based on the symptoms. Doc-Bot is one of the chatbots that patients use for medical assistance [43]. Not only do the chatbots provide individual assistance, but they can also help groups or families with therapy sessions which can be useful for various treatment [17]. A survey of chatbots provides a detailed view of the challenges related to chatbots in the healthcare sector. The survey was articulated from 40 different articles [28]. The chatbot was considered reliable and helpful in terms of medical assistance in a survey conducted by Crutzen [9]. However, chatbots use patients' data to provide correct responses, which leads to privacy and security invasion. For this purpose, we will further discuss privacy and security issues in healthcare chatbots.

Privacy and Security of Healthcare Chatbots

Privacy and security are important aspects when designing any component. With security comes threat and vulnerability, which can be termed a risk for companies as there are chances of the system getting hacked. In terms of chatbots, especially in the healthcare sector, where the system processes user data to function, it is very important to protect it. Chatbots use data to learn and make decisions. In the healthcare sector, the data is sensitive as it contains users' personal information. Users, on the other hand, are not aware of how confidentiality is maintained while communicating with the chatbot. This gives rise to privacy risks for the users as the data is shared with the chatbot. Therefore, it is essential to understand how the data is stored or shared by the conversational agents [16].

There are recent studies that explore various aspects related to privacy and security concerns in chatbots [14, 23, 20, 37]. Jian et al. analyze the trust factor while interacting with the chatbots and proves that there are no notable differences in terms of trust between human to human, human to machine, in general [19]. However, McKnight et al. highlighted that there should be a difference in trust when communicating with humans and with machines. The study mentioned that there is a need to separate trust factors when dealing with people and systems [26]. Large et al. mentions that trust should be considered the factor by which people consider it secure without any harmful impact on them. The study also mentions that trust is an important aspect that must be considered when communicating with the user [22]. Folstad et al. conducted an interview study to determine the trust component in chatbot usage services. The study showed that chatbots were helpful and provided accurate medical help, which enhanced the trust factor in users [14]. Laumer et al. emphasized that the more the level of trust in the system less is the overall privacy concern of the users [23].

To further understand the challenges, we conducted a systematic literature review to explain how healthcare chatbots secure patient data while communicating with them and discuss the factors contributing to it.

METHODS

Two research questions guided our systematic review.

Search	N = 1836	Database search and Title Screening
Screening	N = 312	Abstract Screening
	N = 40	Full-text Screening
Analysis	N = 40	Thematic Analysis

Table 1. A Snapshot of the Data Collection, Screening, and Analysis Methodology Along with the number of Papers Screened in Each Stage of the Literature Review.

- RQ1: In what capacities are chatbots used in the healthcare sector?
- RQ2: What are the current security and privacy measures used in healthcare chatbots?

The systematic literature review will be conducted in January 2022 and includes a corpus of 40 papers collected from different digital libraries. The literature review comprised of six steps: (i) database search, (ii) title screening, (iii) abstract screening, (iv) full-text screening, (v) data extraction, and (vi) thematic analysis. Table 1 provides an overview of the study methodology. Papers were included if they met the following criteria: (1) Published in a peer-reviewed publication, (2) Published in English, (3) Focused on the security and privacy aspects of data in healthcare organizations, (4) The papers focused on healthcare chatbots. We excluded the papers if (1) Papers were works in progress, (2) Papers did not include healthcare chatbots in general, (3) The paper was abstract and entire.

Database Search and Title Screening

We used nine databases: ACM Digital Library, IEEExplore, Google Scholar, Science Direct, PubMed, CHINAHL, MEDLINE, PsychINFO, Sage Journals. The search string was built using keyword terms: chatbot, healthcare, privacy, and security. The keywords in each search varied according to the databases. We also used filters for a search, like if it is published in English. Our initial search led to a total of 1836 papers. The search was carried on using the keywords mentioned above in the title and anywhere else in the paper.

Abstract Screening

Out of the collected papers, we then went through the abstract of each paper to evaluate and filter based on healthcare systems. The abstract screening led to 312 papers in our paper repository.

Full-text Screening

When the titles and abstract appeared relevant, the full text was read. Then, each research paper was assessed to determine its relevance to our research topic by reviewing the full text. This led to a corpus of 40 papers on which we conducted a detailed analysis.

Thematic Analysis

We reviewed the abstract, methods, results, discussion, and conclusion of the 40 collected papers obtained from full-text screening to perform a thematic analysis. We evaluated each paper to determine the theme and provided technological solutions proposed to protect user data. We focused on mutually exclusive to cover these papers' diverse research focus.

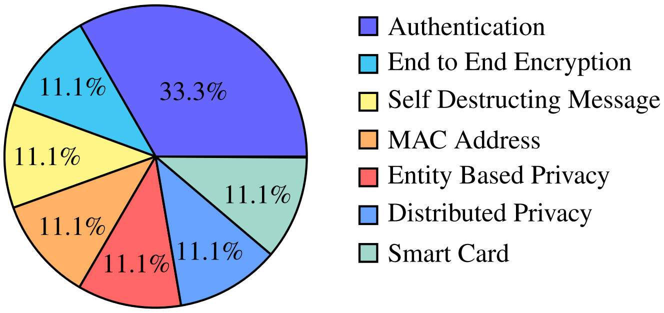

Figure 1. Pie-chart Showing the Distribution of the Technical Solution Papers Based on the Thematic Analysis

RESULTS AND DISCUSSIONS

The papers focused on technology-based solutions for chatbot privacy and security in the healthcare sector. To understand further, we classified the technical solutions proposed by the authors. Figure 1 shows the papers' distribution based on the various technological solutions proposed by the authors to enhance the privacy and security of the chatbot in the healthcare sector.

Technical Solutions

Authentication and Authorization

33.3% of the papers discussed the importance of authentication and authorization to protect user data. The study mentioned how two-factor authentication could be used for greater protection of user-related information and the importance of authorization in chatbots when dealing with user data [16, 31]

End-to-End Encryption

Another critical focus on the technological solution (11.1%) found in our collected sample was on End-to-End Encryption. End-to-End Encryption is a communication system where only the intended sender and receiver can access the message. It enforces encryption by allowing only the authorized user to read the message. Hasal et el. proposes to use an encryption algorithm like the RSA algorithm. In this technique, the user will generate a public and private key in which the public key will be used for encryption, and the private key will be used for decryption. This algorithm ensures that users can communicate with the chatbot using a private key that is known only to the users [16].

Self Destructing Messages

11.1% of the papers discussed self-destructing messages. This can be used when sensitive PII(Personally identifiable information) is transmitted. The idea of this technique is that the highly confidential data should be removed after a particular period so that data privacy is maintained. This technique can be considered a good practice when communicating with chatbots [16].

MAC Address Authentication

11.1% papers discussed authentication and encryption. However, Hasal et al., in their paper, discussed how MAC address authentication could be used as the first form of authentication compared to the traditional way of authentication like username, password, biometric authentication, etc. The study mentioned that the MAC address is tied to the machine-specific and can only be accessed by authorized users. So if the user uses chatbots on a different machine, the chatbot won't run, and this way, we can ensure that only legitimate users can communicate with the chatbots [15].

Entity Based Privacy Preservation

Biswas, in their paper, discusses a new approach to preserving privacy by using entities. The study focuses on entities for preserving the privacy of the users. The author designed a Privacy-Preserving Chat Module (PPCM) module using NLP technology. The design of this solution requires two steps-first is filtering, which is applied to the user query to extract entities, and then the second step where the developed module tries to analyze the original user query to give a natural response to the user back. The filtering step avoids sending valuable information from the query at the back end to avoid privacy invasion [6].

Distributed Privacy Preservation based on Searchable Encryption

Another technique in the sample study discusses an approach where it is possible to protect privacy without knowing the underlying design and techniques used to build the chatbot. Biswas, in their study, proposes searchable encryption implemented on the server-side to preserve user privacy. The technique enables the server not to disclose the original information and search based on encrypted text. The solution allows encrypting the user query using a public key or symmetric key algorithm [6].

Smart-card-enabled Privacy-Preserving E-prescriptions Systems

11.1% of the papers discuss how Smart cards play a crucial role in chatbot security. Smart cards are useful and considered compact repositories that can store users' medical information like the disease user is suffering from, medical history, medicinal intake, etc. This allows the users to authenticate with the card and prevents any disclosure of personal information [35].

Overviews

20% studies focused on the trust concerns that users have when communicating with the chatbots [4, 18, 48, 14, 23, 47, 49, 36]. Rai, in their paper, mentions the need to protect the data in transit using Pseudonymization [34]. 12.5% papers conducted a study to analyze the security and privacy aspects related to chatbots in healthcare. They found that there is still a need to research more in this aspect as a majority of the applications do not provide security aspects in detail [25, 51, 41, 31, 29]. Schmidlen et al. conducted a study to evaluate if users are comfortable in using chatbots for healthcare. The results show that users supported using chatbot and were willing to share information [38]. 5% studies build a framework in their study for healthcare-specific chatbots to ensure privacy and security of user data [11, 46]. 10% studies focused on how building chatbots using artificial intelligence can impact users' experience overall [8, 27, 30, 10]. Bruggemeier and Lalone mention that users' perception in using chatbots and also highlight how privacy prompts can impact users in general [7]. 5% of the studies talked about healthcare chatbots in general [45, 21]. 10% of the studies focused on the design principles of chatbots and suggested measures to build a secure chatbot application [13, 39, 50, 40].

Addressing the Research Questions

We conducted a systematic literature review to understand healthcare chatbots' current security and privacy-related aspects. In addition, we analyzed a total of 40 papers to get insight into how chatbots are designed, developed, and used by the end-users. Through this study, we focused on two research questions discussed in detail in the section below.

RQ1: In what capacities are chatbots used in the healthcare sector?

Our first research question guided how chatbots are used in the healthcare sector. Results show that chatbots provide medical services to users online. The services include prediction of disease, medicinal consultation, therapy, etc. Results also show that the usage of chatbot services has increased considerably due to the pandemic.

RQ2: What are the current security and privacy measures used in healthcare chatbots?

Our second research question focused on this paper's primary aspect, the privacy and security component in general. We found that security and privacy are considered essential aspects when dealing with chatbots in healthcare. The result shows there are technical solutions suggested and implemented to protect the user data. Also, some studies focused on the trust factor and how comfortable users are in communicating with the chatbot. Finally, some studies gave an overview of the overall chatbots in healthcare in general and studied how effective they are in providing medical help.

IMPLICATIONS

We acknowledge the contribution of these previous works toward enhancing the privacy and security of chatbots in healthcare services. However, we note that more research is needed to understand privacy and security challenges in healthcare chatbots fully.

Ethical Implications

Healthcare chatbots are still growing as some users might or might not be comfortable communicating with the chatbot about medical help. While in-person visits ensure privacy and security of sensitive data, as medical professionals cannot share the data, there is no such way that users can ensure privacy with chatbots. Furthermore, many chatbots in the United States do not fall under HIPAA compliance which implies that the users' data can be shared, sold, or stored in the systems. Also, the Pandemic has led to a rise in the usage of healthcare-related chatbots, where users share their medical data without knowing how the data is used after the conversation with a chatbot. Also, privacy-focused laws need to be considered on how chatbots should be used and ensure that there is ethical use of users' data [44].

Addressing User Concerns

The present research shows that the majority have focused on understanding the design of healthcare chatbots. However, patients' perspectives appear to be largely overlooked. Security and privacy requirements should be informed and driven primarily by the desires of patients about their data. Patients are also the most directly impacted by security breaches. More research is required to find and analyze the gaps in patients' understanding of the implications of a security breach to their data. Research is also necessary to understand how much (or how little) trust patients place in their healthcare organizations in protecting their personal data [42].

Accountability Implications

Healthcare services and organizations are responsible for providing medical assistance to patients and ensuring that patients' data is kept hidden from the outside world. Nevertheless, in the case of working with chatbots, there is no such accountability of who should take care of the aspects mentioned earlier. There are no holistic laws and regulations that define patients' security and privacy aspects. HIPAA (Health Insurance and Portability and Accountability Act) in the United States is the act that is used to protect patient's data, but not all chatbots are HIPAA compliant. There is a need to have a regulatory body that governs how the data should be used. Also, there is a need to regulate the ethical use of artificial intelligence products, which includes chatbots to preserve the patient data [24]

Comprehensive Security Approach

With an increase in usage of healthcare chatbots, it is necessary to build these agents using more advanced technology like- natural language processing, machine learning, artificial intelligence. Given that the chatbots provide medical help online and are considered to act as medical professionals, it is essential to design the chatbot such that there is no harm to the patient's health. Our study found that only a few studies mentioned patient safety. Analyzing the user input before making any decision is essential. There are chances that the algorithm working on the back end does not provide the expected response to the patients, leading to severe repercussions. We need more stringent algorithms that can evaluate and provide recommendations to the patients, just like medical professionals [21].

FUTURE WORK AND LIMITATIONS

The main limitation of the healthcare chatbot is in the area of being transparent with the usage of patient data. For example, none of the chatbots share how they are processing the data, who or how many are given access to data, and whether the data is sold. Hence it is difficult to evaluate privacy and security risk as we do not have this information. With the pandemic, chatbots are continuously evolving in providing medical assistance to patients, which needs to be analyzed as personal data is exposed. The future of healthcare chatbots seems to increase; however, data protection, security, and privacy need to be emphasized, and stringent measures to protect them.

CONCLUSION

Healthcare chatbots will become an integral part of our lives, so privacy and security of user data will also be crucial for adopting these chatbots. Another factor that plays an important role is user trust and concerns about using chatbots for medical reasons. We conducted a detailed systematic literature review to study the current research after collecting 1836 papers and thematically analyzing 40 of them. These research articles were published and available over digital libraries: ACM DL, Google Scholar, SSRN, ScienceDirect, IEEE Xplore, PubMed, and MEDLINE. We examined how patients' data is vulnerable when communicating with healthcare chatbots. We found that current research focuses primarily on technological solutions like authentication, authorization, and encrypting user data end to end while understudying the user risk perceptive of privacy and security. We conclude with actionable recommendations from the rich literature we studied that can enhance the privacy and security aspects of chatbots in the healthcare sector.

ACKNOWLEDGEMENT

We would like to acknowledge the Secure Reality Laboratory and the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Laboratory at the University of Denver. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.

REFERENCES

[1] Sameera A Abdul-Kader and John C Woods. 2015. Survey on chatbot design techniques in speech conversation systems. *International Journal of Advanced Computer Science and Applications* 6, 7 (2015).

[2] Eleni Adamopoulou and Lefteris Moussiades. 2020. Chatbots: History, technology, and applications. *Machine Learning with Applications* 2 (2020), 100006.

[3] B Balatamoghna and B Nagajayanthi. 2022. Enhancement of Productivity Using Chatbots. In *Futuristic Communication and Network Technologies*. Springer, 885–892.

[4] Rahime Belen Sağlam, Jason RC Nurse, and Duncan Hodges. 2021. Privacy Concerns in Chatbot Interactions: When to Trust and When to Worry. (2021).

[5] Urmil Bharti, Deepali Bajaj, Hunar Batra, Shreya Lalit, Shweta Lalit, and Aayushi Gangwani. 2020. Medbot: Conversational artificial intelligence powered chatbot for delivering tele-health after covid-19. In *2020 5th international conference on communication and electronics systems (ICCES)*. IEEE, 870–875.

[6] Debmalya Biswas. 2020. Privacy Preserving Chatbot Conversations. In *2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*. IEEE, 179–182.

[7] Birgit Brüggemeier and Philip Lalone. 2022. Perceptions and reactions to conversational privacy initiated by a conversational user interface. *Computer Speech & Language* 71 (2022), 101269.

[8] Yang Cheng and Hua Jiang. 2020. How do AI-driven chatbots impact user experience? Examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. *Journal of Broadcasting & Electronic Media* 64, 4 (2020), 592–614.

[9] Rik Crutzen, Gjalt-Jorn Y Peters, Sarah Dias Portugal, Erwin M Fisser, and Jorne J Grolleman. 2011. An artificially intelligent chat agent that answers adolescents' questions related to sex, drugs, and alcohol: an exploratory study. *Journal of Adolescent Health* 48, 5 (2011), 514–519.

[10] Kerstin Denecke, Alaa Abd-Alrazaq, and Mowafa Househ. 2021a. Artificial intelligence for chatbots in mental health: Opportunities and challenges. *Multiple Perspectives on Artificial Intelligence in Healthcare* (2021), 115–128.

[11] Kerstin Denecke, Alaa Abd-Alrazaq, Mowafa Househ, and Jim Warren. 2021b. Evaluation Metrics for Health Chatbots: A Delphi Study. *Methods of Information in Medicine* 60, 05/06 (2021), 171–179.

[12] Walid El Hefny, Alia El Bolock, Cornelia Herbert, and Slim Abdennadher. 2021. Chase Away the Virus: A Character-Based Chatbot for COVID-19. In *2021 IEEE 9th International Conference on Serious Games and Applications for Health (SeGAH)*. IEEE, 1–8.

[13] Ahmed Fadhil and Gianluca Schiavo. 2019. Designing for health chatbots. *arXiv preprint arXiv:1902.09022* (2019).

[14] Asbjørn Følstad, Cecilie Bertinussen Nordheim, and Cato Alexander Bjørkli. 2018. What makes users trust a chatbot for customer service? An exploratory interview study. In *International conference on internet science*. Springer, 194–208.

[15] Richki Hardi, Ahmad Naim Che Pee, and Nanna Suryana Herman. Enhanced Security Framework On Chatbot Using Mac Address Authentication To Customer Service Quality. (????).

[16] Martin Hasal, Jana Nowaková, Khalifa Ahmed Saghair, Hussam Abdulla, Václav Snášel, and Lidia Ogiela. 2021. Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience* (2021), e6426.

[17] Becky Inkster, Shubhankar Sarda, and Vinod Subramanian. 2018. An empathy-driven, conversational artificial intelligence agent (Wysa) for digital mental well-being: real-world data evaluation mixed-methods study. *JMIR mHealth and uHealth* 6, 11 (2018), e12106.

[18] Carolin Ischen, Theo Araujo, Hilde Voorveld, Guda van Noort, and Edith Smit. 2019. Privacy concerns in chatbot interactions. In *International Workshop on Chatbot Research and Design*. Springer, 34–48.

[19] Jiun-Yin Jian, Ann M Bisantz, and Colin G Drury. 2000. Foundations for an empirically determined scale of trust in automated systems. *International journal of cognitive ergonomics* 4, 1 (2000), 53–71.

[20] Dharun Lingam Kasilingam. 2020. Understanding the attitude and intention to use smartphone chatbots for shopping. *Technology in Society* 62 (2020), 101280.

[21] Liliana Laranjo, Adam G Dunn, Huong Ly Tong, Ahmet Baki Kocaballi, Jessica Chen, Rabia Bashir, Didi Surian, Blanca Gallego, Farah Magrabi, Annie YS Lau, and others. 2018. Conversational agents in healthcare: a systematic review. *Journal of the American Medical Informatics Association* 25, 9 (2018), 1248–1258.

[22] David R Large, Kyle Harrington, Gary Burnett, Jacob Luton, Peter Thomas, and Pete Bennett. 2019. To please in a pod: employing an anthropomorphic agent-interlocutor to enhance trust and user experience in an autonomous, self-driving vehicle. In *Proceedings of the 11th international conference on automotive user interfaces and interactive vehicular applications*. 49–59.

[23] Sven Laumer, Christian Maier, and Fabian Tobias Gubler. 2019. Chatbot acceptance in healthcare: Explaining user adoption of conversational agents for disease diagnosis. (2019).

[24] David D Luxton. 2020. Ethical implications of conversational agents in global public health. *Bulletin of the World Health Organization* 98, 4 (2020), 285.

[25] Richard May and Kerstin Denecke. 2021. Security, privacy, and healthcare-related conversational agents: a scoping review. *Informatics for Health and Social Care* (2021), 1–17.

[26] D Harrison Mcknight, Michelle Carter, Jason Bennett Thatcher, and Paul F Clay. 2011. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on management information systems (TMIS)* 2, 2 (2011), 1–25.

[27] Madison Milne-Ives, Caroline de Cock, Ernest Lim, Melissa Harper Shehadeh, Nick de Pennington, Guy Mole, Eduardo Normando, Edward Meinert, and others. 2020. The effectiveness of artificial intelligence conversational agents in health care: systematic review. *Journal of medical Internet research* 22, 10 (2020), e20346.

[28] Joao Luis Zeni Montenegro, Cristiano André da Costa, and Rodrigo da Rosa Righi. 2019. Survey of conversational agents in health. *Expert Systems with Applications* 129 (2019), 56–67.

[29] Grazia Murtarelli, Anne Gregory, and Stefania Romenti. 2021. A conversation-based perspective for shaping ethical human–machine interactions: The particular challenge of chatbots. *Journal of Business Research* 129 (2021), 927–935.

[30] Tom Nadarzynski, Oliver Miles, Aimee Cowie, and Damien Ridge. 2019. Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study. *Digital health* 5 (2019), 2055207619871808.

[31] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. 2020. Security and privacy of mHealth applications: a scoping review. *IEEE Access* 8 (2020), 104247–104268.

[32] Kyo-Joong Oh, Dongkun Lee, Byungsoo Ko, and Ho-Jin Choi. 2017. A chatbot for psychiatric counseling in mental healthcare service based on emotional dialogue analysis and sentence generation. In *2017 18th IEEE International Conference on Mobile Data Management (MDM)*. IEEE, 371–375.

[33] Bangkok Post. 2017. The Chatbot will Advise you now. *Bangkok Post* (2017), 1–11.

[34] Bipin Kumar Rai. Pseudonymization based Mechanism for Security and Privacy of Healthcare Information System. (????).

[35] Bipin Kumar Rai and AK Srivastava. 2014. Security and Privacy issues in healthcare Information System. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)(ISSN 2278-6858)* 3, 6 (2014).

[36] Lova Rajaobelina, Sandrine Prom Tep, Manon Arcand, and Line Ricard. 2021. Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychology & Marketing* 38, 12 (2021), 2339–2356.

[37] Alexandra Rese, Lena Ganster, and Daniel Baier. 2020. Chatbots in retailers' customer communication: How to measure their acceptance? *Journal of Retailing and Consumer Services* 56 (2020), 102176.

[38] Tara Schmidlen, Marci Schwartz, Kristy DiLoreto, H Lester Kirchner, and Amy C Sturm. 2019. Patient assessment of chatbots for the scalable delivery of genetic counseling. *Journal of genetic counseling* 28, 6 (2019), 1166–1177.

[39] Abubakr Siddig and Andrew Hines. 2019. A Psychologist Chatbot Developing Experience.. In *AICS*. 200–211.

[40] Amela Softić, Jasmina Baraković Husić, Aida Softić, and Sabina Baraković. 2021. Health chatbot: design, implementation, acceptance and usage motivation. In *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 1–6.

[41] Scott Stiefel. 2018. The chatbot will see you now: protecting mental health confidentiality in software applications. *Colum. Sci. & Tech. L. Rev.* 20 (2018), 333.

[42] Faiza Tazi, Josiah Dykstra, Prashanth Rajivan, and Sanchari Das. 2021. SOK: Evaluating Privacy and Security Vulnerabilities of Patients' Data in Healthcare. In *proceedings of the 11th International Workshop on Socio-Technical Aspects in Security and Trust STAST*.

[43] Amiya Kumar Tripathy, Rebeck Carvalho, Keshav Pawaskar, Suraj Yadav, and Vijay Yadav. 2015. Mobile based healthcare management using artificial intelligence. In *2015 International Conference on Technologies for Sustainable Development (ICTSD)*. IEEE, 1–6.

[44] Aditya Nrusimha Vaidyam, Hannah Wisniewski, John David Halamka, Matcheri S Kashavan, and John Blake Torous. 2019. Chatbots and conversational agents in mental health: a review of the psychiatric landscape. *The Canadian Journal of Psychiatry* 64, 7 (2019), 456–464.

[45] M Vijayarani and G Balamurugan. 2019. Chatbot in Health Care–a review. *RGUHS Journal of Nursing Sciences* 9, 1 (2019).

[46] Giovanna Nunes Vilaza and Darragh McCashin. 2021. Is the Automation of Digital Mental Health Ethical? Applying an Ethical Framework to Chatbots for Cognitive Behaviour Therapy. *Frontiers in Digital Health* 3 (2021).

[47] Weiyu Wang and Keng Siau. 2018a. Living with Artificial Intelligence–Developing a Theory on Trust in Health Chatbots. In *Proceedings of the Sixteenth Annual Pre-ICIS Workshop on HCI Research in MIS*.

[48] Weiyu Wang and Keng Siau. 2018b. Trust in health chatbots. (2018).

[49] Angelina Widener and Sohye Lim. 2020. Need to belong, privacy concerns and self-disclosure in AI chatbot interaction. *Journal of Digital Contents Society* 21, 12 (2020), 2203–2210.

[50] Lu Xu, Leslie Sanders, Kay Li, James CL Chow, and others. 2021. Chatbot for Health Care and Oncology Applications Using Artificial Intelligence and Machine Learning: Systematic Review. *JMIR cancer* 7, 4 (2021), e27850.

[51] Winson Ye and Qun Li. 2020. Chatbot Security and Privacy in the Age of Personal Assistants. In *2020 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 388–393.