International Journal of Business and Management Invention (IJBMI)
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 13 Issue 7 || July, 2024 || PP: 28-32

Chatbot Security: Protecting User Data and Privacy

Dr.B.Keerthana
Assistant Professor,
Department of Management Studies, Sri Sai Ram Engineering College

Vaishali C
I year MBA, Department of Management Studies,
Sri Sai Ram Engineering College

Anitha S
I year MBA, Department of Management Studies,
Sri Sai Ram Engineering College
West Tambaram, Chennai-600 044

ABSTRACT*: In the modern era of technology, chatbots have gained immense popularity due to their convenience and efficiency in providing information and assistance. These bots are specifically designed to interact with users and offer helpful information or assistance based on their programming. By utilizing artificial intelligence, chatbots can comprehend and respond to user queries or commands. However, as the field continues to evolve, it is crucial for the conversational AI community to remain vigilant of any potential vulnerabilities in existing architectures and how attackers could exploit them. To ensure statistical significance and robust analysis of the research findings, a sample size of 150 participants were selected for this study. The analysis of the study identified the security issues faced by users. The listed issues were discussed and appropriate alternatives were suggested.*

KEYWORDS:
Chatbot, security, data protection, artificial intelligence

I. INTRODUCTION

The chatbot concept can be traced back to Alan Turing's vision of intelligent machines in the 1950s. Since then, artificial intelligence has advanced significantly, leading to the development of super intelligent supercomputers like IBM Watson. Initially, the phone tree served as the first chatbot, guiding customers through automated customer service processes by selecting options. However, advancements in technology and the refinement of AI, ML, and NLP have transformed this model into interactive onscreen chats. This evolution continues to progress. Today, businesses leverage digital assistants to enhance customer interactions, offering more convenient and effective communication directly from customers' digital devices.AI chatbots present ethical dilemmas including privacy, consent, transparency, and accountability, despite their efficiency. It is imperative to solely gather essential information and safeguard it against any form of misuse, all while obtaining consent from customers. Additionally, customers must be well-informed about their interactions with AI systems.

OBJECTIVES:
To identify the security issues faced by Chatbot users.

II. RESEARCH PURPOSE AND RESEARCH QUESTIONS

RESEARCH PURPOSE
The aim of this research is to identify the security challenges encountered by users and vulnerabilities in chatbots. Additionally, it explores how attackers exploit the data. Furthermore, the main goal of this study is to provide recommendations for addressing these issues

RESEARCH QUESTIONS
1. Did you face any security issues while using chatbots ?
2. In your opinion, biggest threat for security of user data using chatbots
3. In your opinion, what are the role of users in ensuring security of data while using chatbots ?
4. What are the security measures that make you feel more comfortable?

III. REVIEW OF LITERATURE

Chatbots are becoming increasingly prevalent in various domains due to their efficiency, 24/7 availability, and user-friendly nature for providing instructions to computers.The evolution of chatbot design techniques is ongoing, making it increasingly challenging to differentiate between interactions with a human and a chatbot. Certain chatbots are now capable of providing mental health support, necessitating a high level of conversational proficiency. Despite this, a few chatbots have managed to deceive up to 3 out of 12 judges into believing they were human. Major tech companies have access to vast amounts of conversational data and the means to hire skilled programmers. As chatbot design techniques continue to advance, the speech of chatbots will become more human-like. Consequently, chatbots present on social media platforms will become more reliable, potentially exerting even greater influence on people's opinions.

As previously mentioned, chatbots are essentially programmed systems that facilitate input and output, and there are established guidelines for creating and operating them. However, the use of chatbots also entails significant responsibility and cybersecurity risks. In many instances, chatbots handle sensitive information, necessitating the implementation of robust security measures. Communication with chatbots occurs through existing channels and protocols, which generally do not pose new security concerns as they have already been identified and effectively addressed. Nevertheless, it is important for users to refrain from sharing personal data while engaging in conversations with chatbots, as not all chatbots communicate through encrypted channels.

Certain security issues arise from the storage of communications and user data. The challenge lies in the fact that communication data holds immense value, leading many companies to retain past conversations. While data can be encrypted on servers, machine learning algorithms cannot be trained on encrypted data, rendering the results meaningless. Additionally, natural language processing tools are not equipped to learn from encrypted data. Consequently, there are instances when communication becomes exposed and readable. Companies must adhere to regulations such as the GDPR and similar rules when handling personally identifiable information (PII), ensuring that discussions involving PII are not shared among employees or external parties. From a broader perspective, chatbots record and learn from previous conversations, subsequently utilizing words, phrases, and complete utterances in future interactions.

Another concern is that chatbots can operate on third-party conversational interfaces and networks, such as Facebook Messenger, Viber, Facebook-WhatsApp, Twitter, Facebook, LinkedIn, and others. Each of these platforms has distinct policies regarding user ownership and company ownership of data when users utilize their services. For instance, there were over 300,000 active users on a particular platform.

Communication in human language is a crucial method for conveying emotions, thoughts, and issues among individuals. As chatbots gather information from users, they have the ability to mimic the user's way of speaking. An instance of this is Microsoft's chatbot 'Tay', which transformed from a typical teenage girl into a chatbot expressing anti-Semitic, racist, and sexist views within a short span of sixteen hours. Another Microsoft chatbot, 'Zo', also adopted some inappropriate behaviours.

Omari et al., (2013) Asserted that some researchers have tried to pinpoint the key factors behind varying degrees of compliance with information security policy. Academic literature and information security institutes' reports on information security policy compliance have been reviewed in this regard.

Hina and Dominic (2017) Recommend that ISA and training programs have an essential part to play in adopting protective technologies, developing a security culture, and compliance with organisational policies. Adaptable awareness programs can be tailored to enhance the ever-evolving organizational security demands .

Goode et al. (2018) Highlighted the crucial role of Information Security Awareness in Information Security Policy Compliance. In their view, employees should be able to detect(awareness) security threats and demonstrate a degree of knowledge about information security and be up to date or stay abreast with security technology and clearly understand what it is all about. This definition is in line with the notion that information security awareness (ISA) refers to a state where employees in a business entity are cognizant of and ideally have a buying to the security mission.

Nair and Johnson (2018) Chatbot applications are now regarded as modern-day browsers**.** Chatbot technology is perceived as the future of communication between humans, webpages, and applications.

Haingura (2019) The human factor in information security refers to employee actions that can lead to a breach in IS. These actions result from poor security conduct, negative attitude towards ISP, unhappy users, theft, and insufficient knowledge.

Caldarini, Jaf & McGarry (2022) A chatbot responds using the same applications, creating a back-and-forth conversation The use of chatbots will help enforce compliance and raise awareness at the same time. Further to

this, the term chatbot dates back to the Nineties. It implies a computer program that intends to simulate and reproduce a smart interaction with a user.

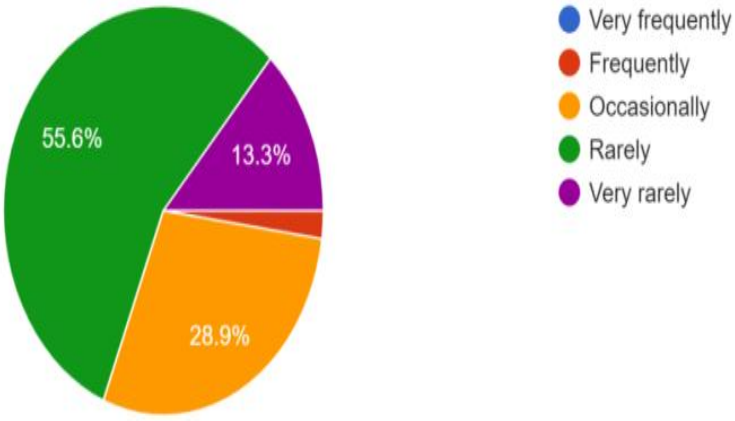
RESEARCH METHODOLOGY

- In this study descriptive research is used. A sample of 44 respondents were selected through simple random sampling.
- Percentage analysis was used for describing the facts chosen for the study.

IV. DATA ANALYSIS

4.1 Security issues while using Chatbots

Figure 4.1 showing security issues while using Chatbots



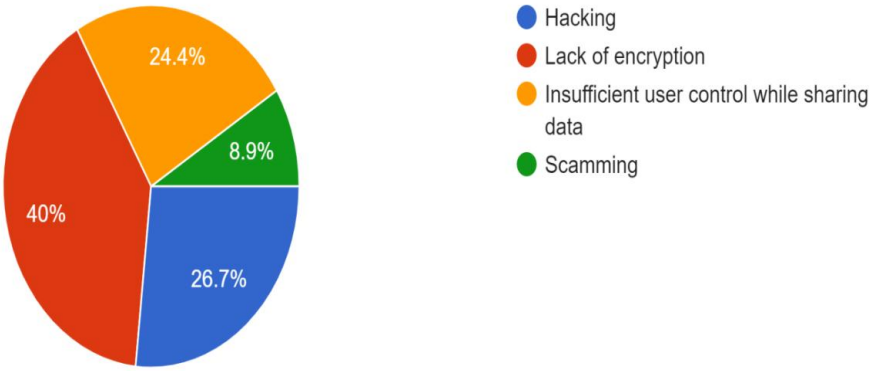
SOURCE : PRIMARY DATA (Questionnaire)

INTERPRETATION :

The above figure shows that how frequently the respondents' face security issues while using chatbot. Here, majority respondents faces issues rarely 55.6%. 28.9% respondents faces occasionally. 13.3% faces very rarely and 2.2% faces issues frequently.

4.2 Biggest threat for security of user data using chatbots

Figure 4.2 showing biggest threat for security of user data using chatbots

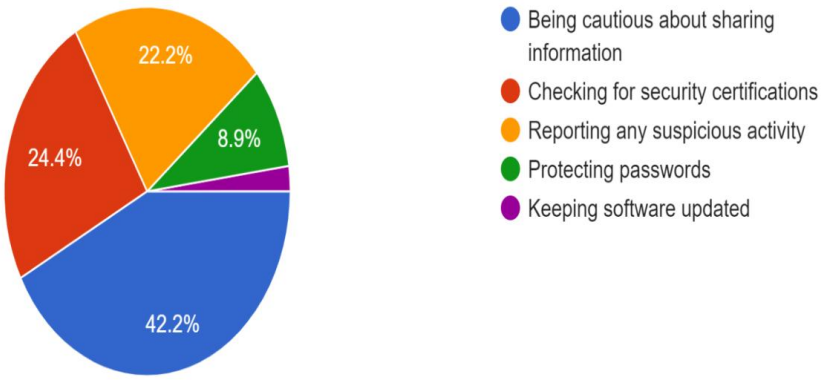


SOURCE : PRIMARY DATA (Questionnaire)

INTERPRETATION :
The above figure shows the perception of respondents about the biggest threat for security of user data while using Chatbots. Here, the major respondents mentioned that there is lack of encryption which is 40%. Next to that 26.6% mentioned that is hacking. 24.4% mentioned insufficient user control while sharing data and 8.9% mentioned about scamming.

4.3 Role of users in ensuring security of data while using chatbots

Figure 4.3 Role of users in ensuring security of data while using chatbots

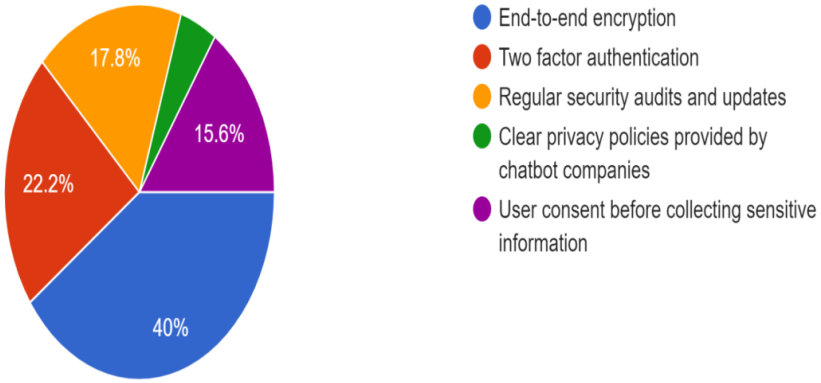


SOURCE : PRIMARY DATA (Questionnaire)

INTERPRETATION :
The above figure shows about the respondents' perception towards the role of users in ensuring security of data while using chatbots. Here, the majority of respondents which is 42.2% feels that the users should be cautious while sharing information. 24.4% respondents feels that the users should check for security certifications.22.2% votes for reporting any suspicious activities. 8.9% for protecting passwords and 2.2% for keeping software updated.

4.4 Security measures that make users feel comfortable

Figure 4.4 showing the security measures that make users feel comfortable



SOURCE : PRIMARY DATA (Questionnaire)

INTERPRETATION :

The above figure shows about the respondents perception towards security measures that makes users feel more comfortable. Here, the major respondents which is 40% needs end-to-end encryption. Next to this, 22.2% needs two factor authentication. 17.6% needs regular security audits and updates, 15.6% needs user's consent before collecting sensitive information and 17.8% needs clear privacy policies provided by chatbot companies.

V. SUGGESTIONS

1. Encryption:

Make sure that all communication between the user and the chatbot is securely encrypted using protocols such as HTTPS in order to safeguard against unauthorized access.

2. Two Factor Authentication:

Integrating two-factor authentication (2FA) into chatbots requires the addition of an extra security measure on top of the standard username and password login.

3. Audits:

Perform routine security audits to detect vulnerabilities within the chatbot system and promptly resolve any identified issues.

4. Secure Storage:

Safeguard user information by storing it in protected databases with robust encryption and strict access restrictions to deter unauthorized entry.

VI. CONCLUSION

Chatbots offer undeniable benefits due to their ability to operate 24/7, reduce costs compared to human workers, communicate in natural language, and handle a wide range of tasks. Many individuals find instant messaging more user-friendly than email or web forms. Chatbots and voice assistants can be found on various platforms such as social media, communication platforms, websites, mobile phones, computers, and more. Users interact with chatbots in numerous sectors including banking, healthcare, online shopping, automotive, insurance, airports, and many others. Therefore, ensuring secure communicationwith chatbots is crucial to safeguard user data.

REFERENCES

JOURNAL REFERENCES :

[1]. Edu, J., Mulligan, C., Pierazzi, F., Polakis, J., Suarez-Tangil, G. and Such, J., 2022, October. Exploring the security and privacy risks of chatbots in messaging services. In Proceedings of the 22nd ACM internet measurement conference (pp. 581-588).

[2]. Edu, J., Mulligan, C., Pierazzi, F., Polakis, J., Suarez-Tangil, G. and Such, J., 2022, October. Exploring the security and privacy risks of chatbots in messaging services. In Proceedings of the 22nd ACM internet measurement conference (pp. 581-588).

[3]. Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V. and Ogiela, L., 2021. Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience*, *33*(19), p.e6426.

[4]. May, R. and Denecke, K., 2022. Security, privacy, and healthcare-related conversational agents: a scoping review. Informatics for Health and Social Care, 47(2), pp.194-210.

[5]. Siyongwana, G.M., 2022. The enforcement of end-user security compliance using Chatbot (Doctoral dissertation, Cape Peninsula University of Technology).

[6]. Surani, A. and Das, S., 2022. Understanding privacy and security postures of healthcare chatbots. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. Presented at: CHI (Vol. 22, pp. 1-7).

[7]. Yang, J., Chen, Y.L., Por, L.Y. and Ku, C.S., 2023. A systematic literature review of information security in chatbots. Applied Sciences, 13(11), p.6355.

[8]. Ye, W. and Li, Q., 2020, November. Chatbot security and privacy in the age of personal assistants. In 2020 IEEE/ACM Symposium on Edge Computing (SEC) (pp. 388-393). IEEE.

URL REFERENCES :

1. https://www.oracle.com/chatbots/what-is-a-chatbot/#:~:text=Chatbots%20are%20conversational%20tools%20that,cannot%20be%20replicated%20by%20machines