Chapter 12
Conversational AI Chatbots in Digital Engagement:
Privacy and Security Concerns

Uma S.
Hindusthan College of Engineering and Technology, Coimbatore, India

ABSTRACT

Digital transformation and globalisation have taken the online business to the next frontier, embracing the customer engagements with conversational artificial intelligence or chatbots. Chatbots are deployed across several industries ranging from e-commerce to healthcare. While the advantages of using chatbots are enormous, chatbots also introduce certain pitfalls. A lack of diversity among creators may result in biased responses from the chatbot. Though chatbots are widely used, not all of their security issues are satisfactorily resolved. It causes significant security issues and risks, which needs immediate attention. Many chatbots are built on top of social/messaging platforms, which has its own set of terms and conditions governing data collection and usage. This work gives a detailed analysis of security considerations in the context of communication with bots. This chapter has the potential to spark a debate and draw attention to the issues surrounding data storage and usage of chatbots to protect users.

INTRODUCTION

Face-to-face human interactions are becoming less common, and communication through technology is gaining prominence. Chatbots are machines that replicate interactive human interaction utilizing artificial intelligence (AI), pre-calculated user

DOI: 10.4018/978-1-6684-6234-8.ch012

words, and audio and written signals. Chatbots can process user input and produce outputs. A chatbot usually accepts natural language text as input and produces the most relevant output to the user's input. A chatbot can also be defined as "an online human-computer dialogue system using natural language" (Andrej Godina, 2018). Chatbots constitute an automated dialogue system that can attend to thousands of potential users simultaneously. An artificial messenger, or "bot," allows customers to communicate with a service provider (e.g., a bank, online shopping catalog, or public utility). Chatbots are also often integrated into operating systems as intelligent virtual assistants. Customer support and marketing systems rely on chatbots in social networking hubs and instant messaging (IM) applications.

Artificial intelligence (AI)-based chatbots like Google's LaMDA, Open AI's GPT-3, Meta's BlenderBot, Amazon's Alexa, and Apple's Siri have been trained on billions of documents, giving the concept of "massive data" (O'Leary, 2022). These systems use documents that people create themselves to record the words and connections between words they use when speaking. These chatbot technologies are increasingly becoming part of our daily lives. As a result, businesses are now implementing chatbots into their networks, offering consumers a more efficient and user-friendly experience across many platforms. Retail and e-commerce, learning management systems (LMS), travel and hospitality, sales, marketing, customer relationship management (CRM), banking, financial services, insurance, healthcare, media, and entertainment are some of the other applications of chatbots.

Artificial intelligence is already enabling chatbots in the commercial sector to interact with customers on a far more personal level than the conventional, automated "Press one for admin" phone reply. Voice is becoming more essential in chatbot technology (Andrej Godina, 2018). For example, today's chatbot technology can also answer more complex inquiries orally; Amazon's Alexa, for instance, is a popular AI assistant that works with Amazon's home hub. The reality is that it's often difficult to tell whether the conversation is with a real person or a chatbot.

The advent of chatbots has changed the way people think and live. They are always available and ready to provide service assistance as well as carry out other tasks whenever and wherever people need them. In addition to communication tools, chatbot technology comes with significant IT-related benefits, but it can also entail risks for the organizations using it. There are several security threats associated with the use of chatbots. The existing chatbot solutions are not completely secure, and the organizations using chatbots may get exposed to cyberattacks. Cyberattacks are increasing in number, but detecting and analyzing such attacks requires a lot of knowledge and tools. Information security incidents require experts who can investigate security incidents and have a broad knowledge base. Using a reliable security tool on the Internet is crucial for using these virtual assistants. Such vulnerabilities provide hackers with direct access to an organization's applications,