Safeguarding Privacy in the ChatGPT Era: A Comprehensive Analysis of Data Protection Measures

M.I. Fathima Nihla

Department of Management and IT, Faculty of Management and Commerce, South Eastern University of Sri Lanka

nihla@seu.ac.lk

ABSTRACT

Purpose: With an emphasis on ChatGPT specifically, this study attempts to look into data protection measures in AI-driven conversational models. As artificial intelligence (AI) technology become more ubiquitous in daily life, worries regarding data security and privacy have grown. The study aims to evaluate ChatGPT's present data protection practices, spot potential dangers and weaknesses, and suggest solutions that fit changing user expectations, regulatory requirements, and ethical standards. The main objective is to ensure privacy in the development and application of conversational AI models by bridging the gap between technical breakthroughs and ethical issues.

Design/Methodology/Approach: A thorough approach for reviewing the literature was used, looking at academic studies, industry reports, and legislative frameworks pertaining to cybersecurity, data privacy, and AI ethics. With a focus on ChatGPT-like models, the review summarized findings from earlier research on data safety in conversational AI. The study evaluated the benefits and drawbacks of the state-of-the-art data protection procedures and pinpointed research needs by critically examining the literature. In order to guarantee compliance, the investigation also looked at regulatory requirements like GDPR in relation to AI-driven dialogues.

Findings: The analysis of the literature showed that even with ChatGPT's many data protection features, there are still a number of serious weaknesses, especially when it comes to handling dynamic chats and retaining user data. The main dangers that have been identified include inadequate user control over personal data, inadequate openness in data handling, and unauthorized access to sensitive information. The study also revealed shortcomings in user education about privacy procedures. The report suggested a number of improved approaches to deal with these problems, such as stronger encryption, increased data usage transparency, and better user education initiatives.

ISBN: 978-955-627-030-3

Practical Implications: The study provides stakeholders, legislators, and AI developers with useful suggestions. Through the identification of weaknesses in current data protection protocols, the study offers a path forward for enhancing conversational AI privacy and security protocols. The suggested tactics, which include improved encryption procedures, adherence to changing regulatory requirements, and improved user training, can assist developers in building AI models that are more private-focused and safe. These results also aid in the development of regulatory frameworks that guarantee the appropriate application of AI while protecting user privacy and confidence.

Originality/Value: This work contributes to the literature by concentrating on the data privacy issues that conversational AI models such as ChatGPT face. Although data privacy and AI ethics are extensively researched, this study tackles the particular issues associated with AI-driven dialogues and suggests customized remedies. The study's conclusions offer insightful information to audiences in academia and business, laying the groundwork for further investigation and advancement in the safe application of conversational AI.

Keywords: ***Chatgpt, Data Protection, AI Ethics, Conversational Models, Cybersecurity, Legal Frameworks***

ISBN: 978-955-627-030-3