Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 18–21
DOI: https://doi.org/10.58496/MJCS/2023/004,ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

**Review Article**

# ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information

Maad M. Mijwil[1,*], Mohammad Aljanabi[2], Ahmed Hussein Ali[2],

[1] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[2] *Department of Computer, College of Education, Aliraqia University, Baghdad, Iraq*

**ARTICLE INFO**

Article History
Received 17 Jan 2023
Accepted 28 Jan 2023
Published 1 Feb 2023

Keywords
ChatGPT
Cybersecurity
Medical data
Digitization



## Intro to ChatGPT

OpenAI's ChatGPT is a robust linguistic model. It can be used to generate responses in multiple languages and formats that sound natural because they were trained on a dataset of conversational text. It can be used for activities such as chatbots, language translation, and text completion. ChatGPT's goal is to produce natural-sounding responses to certain questions or situations. It has several potential uses, including but not limited to chatbots, language translation, text completion, and answering questions. It can also be trained to perform particular jobs, such as writing summaries of articles or describing products. It can also be utilised as a source of inspiration for fiction and poetry. It has widespread potential for application, from customer service and the arts to science and academia.

## The significant of ChatGPT

OpenAI's massive language model is called ChatGPT (Conversational Generative Pre-training Transformer). As a result of its natural language processing, language translation, text summarization, conversation production, and other capabilities, it is a versatile tool. The training process for ChatGPT is depicted in Figure 1.

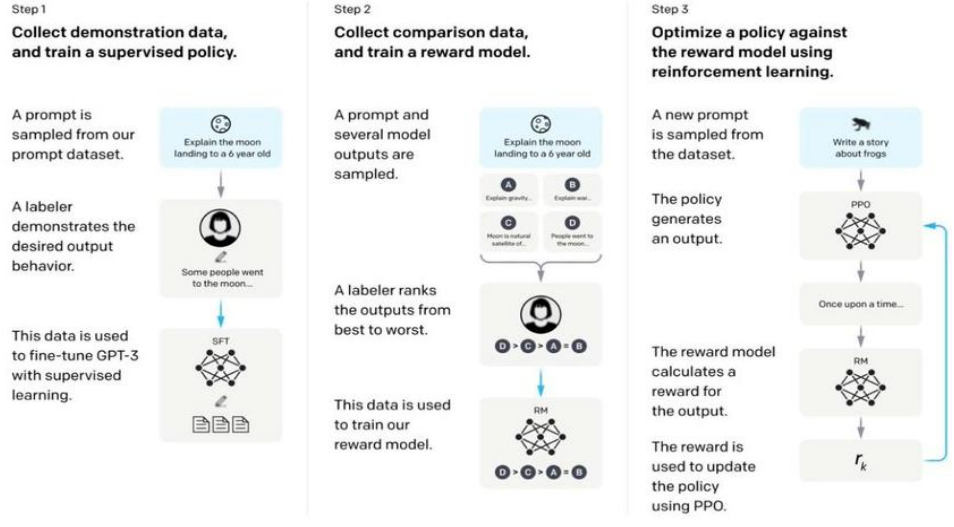


Fig. 1. How ChatGPT is trained [Downloaded from Google].

ChatGPT is a significant language model for a few reasons:

*Corresponding author. Email: mr.maad.alnaimiy@baghdadcollege.edu.iq

**Scale**: There are billions of parameters in this language model, making it one of the most complex available. This permits it to come up with more elaborate and interesting answers to questions.
**Pre-training**: Since ChatGPT has already been trained on a large corpus of conversational data, it can produce natural-sounding output without being fine-tuned for a specific job or dataset.
**Versatility**: ChatGPT has a lot of potential applications across various fields, from customer service and media to education and science.
**Efficiency**: Due to its computational efficiency and ability to run on edge devices, GPT-3 and ChatGPT make it simpler for developers to create apps based on language models.
**Quality**ChatGPT produces natural-sounding, nearly indistinguishable from human-written text.
In sum, ChatGPT is a major step forward for natural language processing and has the potential to affect numerous fields and uses. The ChatGPT [1-4] will be used to draught the remaining portions of this article. This article's major goal is to demonstrate how useful ChatGPT is for generating scripts in the realm of cyber security.

## Cybersecurity in digitization

Cybersecurity refers to the process of preventing harm to or unauthorised access to computer systems, networks, and data that are connected to the internet. The importance of cyber security has grown as more and more of our daily lives, both professionally and personally, are conducted online. As more and more things become digitally connected to the internet and more data is stored and exchanged digitally, it becomes increasingly difficult to safeguard against cyber dangers. Firewalls, encryption, and multi-factor authentication are just some of the security precautions that businesses and people may take to reduce their vulnerability. Another way to shield yourself from exploits is to always use the most recent security fixes for your software and hardware. Digitization is the process of transforming analogue sources of data into their digital counterparts. Digitization has several positive effects.

- Digital information can be more efficiently stored, searched, and shared than paper records can. Productivity gains and improved speed of action may result.
- Organisations can save money thanks to digitization because it reduces the demand for paper and other physical storage materials.
- Digitization can aid in the preservation of priceless cultural artefacts and historical documentation for future generations.
- Increasing accessibility and democratising information, the internet and digital gadgets make digital content available to a larger audience.
- Inspiration: New, state-of-the-art capabilities, such as big data analysis and artificial intelligence, are now available to us thanks to the proliferation of digital information.Improved Capacity to Choose Digitization facilitates real-time data analysis, performance monitoring, and improved decision making.
  As an essential part of today's economy and culture, digitalization is only going to become more important in the years to come.

### Digital health data

Digital health data refers to the collection and use of electronic health information in healthcare, including patient medical records, test results, and other health-related information. The benefits of digital health data include:

- Improved patient care: Digital health data allows healthcare providers to have easy access to a patient's complete medical history and current health status, which can improve the accuracy and quality of care they provide.
- Increased efficiency: Digital health data can help streamline healthcare processes and reduce administrative workload, leading to increased efficiency and cost savings.
- Better coordination of care: Digital health data can facilitate better communication and collaboration among healthcare providers, leading to improved coordination of care for patients.
- Better patient engagement and self-management: Digital health data can help patients better understand their health conditions and treatment options, and enables them to be more involved in their own care.
- Advanced data analytics: Digital health data can be used for advanced analytics such as machine learning, big data analysis, and predictive modeling, which can help identify patterns, trends, and insights that can improve patient outcomes and reduce costs.

However, digital health data also raises concerns about security and privacy. It's important for healthcare organizations to implement strong security measures and comply with relevant regulations to protect patient data. Healthcare workers are

starting to use artificial intelligence (AI) in a variety of ways to improve patient care and make healthcare systems more efficient. Some examples of how AI is being used in healthcare include:

- Diagnostics: AI-powered tools can assist in the diagnosis of diseases by analyzing medical images, such as X-rays and CT scans, and providing information to assist in the diagnostic process.
- Medical imaging analysis: AI-powered algorithms can analyze medical images, such as CT and MRI scans, to identify areas of concern, such as tumors or other abnormalities, which can help radiologists make more accurate diagnoses.
- Predictive modeling: AI can be used to predict patient outcomes and identify those at high risk for certain conditions, such as readmission to the hospital, which can help healthcare providers develop more effective treatment plans.
- Personalized medicine: AI can be used to analyze patient data to identify personalized treatment options that are most likely to be effective for each individual patient.
- Streamline clinical workflows: AI can assist in automating repetitive tasks, such as data entry, scheduling, and appointment reminders, freeing up healthcare workers to focus on other important tasks.
- Remote monitoring: AI-powered devices, such as smartwatches, can be used to remotely monitor patients' vital signs and alert healthcare providers if there are any concerning changes.

**Cybersecurity in the Medical Information**

Protecting medical information is a critical aspect of healthcare, as it is highly sensitive and personal. Medical information includes patient's personal information, medical history, and health records, and its unauthorized disclosure or theft can cause serious harm to patients. Protecting medical information is a critical aspect of cybersecurity in the healthcare industry. Medical information is highly sensitive and personal, and its unauthorized disclosure or theft can cause serious harm to patients. Some of the ways to protect medical information include:

- Encryption: Encrypting medical data can prevent unauthorized access to information, even if it is intercepted or stolen.
- Access controls: Implementing strict access controls, such as multi-factor authentication, can prevent unauthorized individuals from gaining access to medical information.
- Regularly updating software: Keeping software and systems up-to-date with the latest security patches can help protect against known vulnerabilities.
- Network security: Implementing firewalls, intrusion detection and prevention systems, and other network security measures can help protect against cyberattacks.
- Risk management: Regularly assessing and managing potential security risks can help healthcare organizations identify and address potential vulnerabilities before they can be exploited.
- Compliance: Adhering to industry regulations, such as HIPAA, can help ensure that medical information is being handled and protected in accordance with legal and ethical standards.
- Regular security audit: Regularly audit the security infrastructure of the organization to detect any vulnerabilities and risks.
- Employee education: Regularly educate and train employees on security best practices and the importance of protecting medical information.

## Point of view and the future

We have reached ChatGPT's ability to write in an academic and advanced manner and the possibility of creating sections according to the desire of authors through Chat in this platform. In the future, we expect that artificial intelligence will contribute more to assisting researchers in writing scientific articles and will play a major role in developing scientific research.

## Funding

The author's paper does not provide any information on grants, sponsorships, or funding applications related to the research.

## Conflicts of Interest

The author's affiliations, financial relationships, or personal interests do not present any conflicts in the research.

## Acknowledgment

The author acknowledges the research department at the institution for their assistance and technical expertise in conducting this study.

## References

[1] M. M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, H. Al-Shahwani, and ChatGPT, "The Purpose of Cybersecurity in the Digital Transformation of Public Services and Protecting the Digital Environment," Mesopotamian Journal of Cybersecurity, vol. 2023, pp. 1-6, January 2023. Available: https://doi.org/10.58496/MJCS/2023/001

[2] M. M. Mijwil, M. Aljanabi, and ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 65-70, January 2023. Available: https://doi.org/10.52866/ijcsm.2023.01.01.0019

[3] M. M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," Mesopotamian Journal of Cybersecurity, vol. 2022, pp. 1-4, 2022. Available: https://doi.org/10.58496/MJCS/2022/001

[4] M. Aljanabi, M. Ghazi, A. H. Ali, S. A. Abed, and ChatGPT, "ChatGpt: Open Possibilities," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 62-64, January 2023. Available: https://doi.org/10.52866/ijcsm.2023.01.01.0018