Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity

3 authors, including:

Musadaq Hadi
University of Technology, Iraq
10 PUBLICATIONS **61** CITATIONS

Mohammed Najm
University of Baghdad
3 PUBLICATIONS **1** CITATION

Review Article

Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity

Musadaq A. Hadi[1] , Mohammed Najm Abdulredha[2], and E. Hasan[3]

[1]*Control and Systems Engineering Department, University of Technology, Baghdad, Iraq*
[2]*Computer Science Department, University of Baghdad, Baghdad, Iraq*
[3]*Institute for Mathematics Research, University Putra Malaysia, Malaysia*
[3]*Department of Mathematics, University of Baghdad, Al-Jadrriya, Baghdad, Iraq*
(✉) Corresponding Author: Musadaq A. Hadi

Abstract

ChatGPTis an innovative natural language processing (NLP) technology developed by OpenAI. It has revolutionized human-computer interactions by utilizing Machine Learning (ML) and Deep Learning (DL) algorithms. ChatGPT generates a remarkable human-like conversations in response to user input. Consequently, the efficiency of ChatGPT lies in its ability to identify patterns in text, analyze context and produce responses that mimic human conversation. Its use of deep learning techniques which enables it to capture syntactic and semantic structures that resulting in natural-sounding output. Furthermore, its adaptive learning capability allows it to continuously improve and update its language understanding through exposure to a vast amount of user interactions. In this paper, a historical review of ChatGPT is introduced to catch up with the revolution of the Artificial Intelligence (AI) impact on life aspects, economic, financial, military and cybersecurity. Eventually, a comparison is made between ChatGPT versions and other AI platforms to present the effectiveness, weakness and strength points.

Keywords: ChatGPT, Artificial Intelligence, Machine Learning, Chatbot and Cybersecurity

Introduction

OpenAI organization and its efforts in advancing artificial intelligence and natural language processing. OpenAI was founded in December 2015 with the mission of ensuring that Artificial General Intelligence (AGI) benefits all of humanity. OpenAI's early projects, such as OpenAI Gym and OpenAI Universe were focused on reinforcement learning and creating environments for AI agents to learn and interact with. Therefore, these initiatives laid the foundation for OpenAI's future work in developing more sophisticated AI models. The initial breakthrough in natural language processing came with the development of the Generative Pre-trained Transformer (GPT) model. GPT has marked a significant advancement in language generation tasks. Obviously, Elon Mask was the first Chief Executive Officer (CEO) of the company and now Sam Altman is the current CEO and Elon Mask is no longer the CEO of OpenAI (Zhou et al., 2023).

In June 2018, GPT was introduced and trained by OpenAI on a massive corpus of text data and demonstrated impressive language understanding and generation capabilities. Building upon the success of GPT, subsequent versions of the model were released, including GPT-2 in February 2019 and GPT-3 in June 2020. These models showcased the ability to generate coherent and contextually relevant text, attracting widespread attention and interest. After that, the evolution of ChatGPT specifically began with the release of GPT-3 which demonstrated unprecedented language capabilities and prompted further exploration of its potential applications in conversational AI. OpenAI recognized the significance of generating human-like conversations and started fine-tuning GPT-3 for chat-based interactions (Cao et al., 2023).

The feedback process helped OpenAI gather valuable insights and make improvements to the model's performance, accuracy, and safety. As part of OpenAI's commitment to

responsible AI development, a cautious approach was taken to address concerns regarding potential biases, misinformation, and malicious use of the technology. OpenAI has continuously worked on refining ChatGPT, implementing safeguards, and developing moderation techniques to mitigate these risks. The historical development of ChatGPT represents a culmination of OpenAI's ongoing research and innovation in natural language processing. Furthermore, this was merged with a focus on creating AI systems that can engage in human-like conversations and enhance human-computer interactions (Dale, 2020).

ChatGPT is the latest development in Artificial Intelligence (AI) technology widespread large language model within the company open AI. Despite meeting professional and academic standards, ChatGPT is freely accessible to all users. It has revolutionized the field of information technology and currently boasts 57 million active monthly users, with projections of surpassing 100 million users as in Fig. 2. This allows it to accurately interpret user input and generate the appropriate response in real time. This platform has achieved great success among users as it has been rated the most popular application. The fastest growing consumer in the history of the Internet will learn about the features of ChatGPT, how it works and key terms that help during the summary of ChatGPT (Liu et al., 2021).

Many studies have been made in order to highlight the contributions and impacts of ChatGPT on human life especially on AI, financial, military, education and Cybersecurity. ChatGPT had the potential to significantly impact financial affairs worldwide. It can analyze vast amounts of financial data, assist in algorithmic trading, improve risk assessment and fraud detection. Additionally, GPT can enhance customer service through Chatbots, automated content generation, and aid in regulatory compliance. However, ethical considerations and challenges regarding data privacy and algorithmic bias must be carefully addressed for responsible implementation (Cao and Zhai, 2023; Ali and Aysan, 2023; Dowling and Lucey, 2023). Furthermore, ChatGPT and similar AI technologies have significant impacts on the military field. They can assist in intelligence analysis, mission planning, and simulation exercises. Additionally, ChatGPT enables natural language interfaces and enhances the capabilities of autonomous systems. It can also contribute to cybersecurity, training, language translation, and cultural understanding. Ethical considerations and human oversight are crucial in ensuring responsible use of AI in the military (Biswas, 2023; Macey-Dare, 2023; Szabadföldi, 2021; Ding and Dafoe, 2023).

Moreover, ChatGPT brings about substantial changes in the field of education by providing customized learning opportunities and functioning as virtual tutors or assistants. It supports language acquisition, generates and curates educational content, and promotes inclusivity for students with disabilities. Additionally, it offers automated feedback, aids in research, and facilitates information retrieval. Nevertheless, it

is vital to ensure appropriate human guidance and address ethical considerations for responsible integration in education (Rahman and Watanobe, 2023; Lo, 2023; Halaweh, 2023).
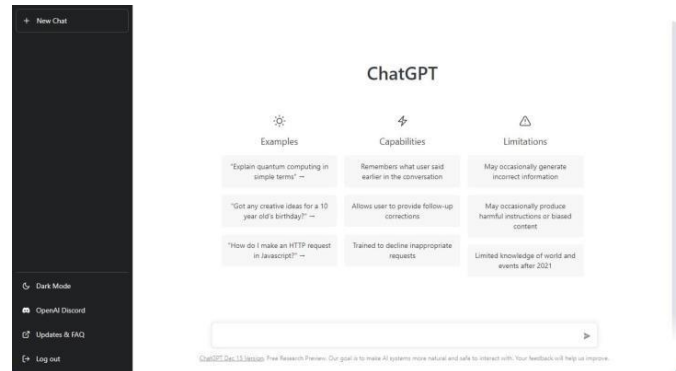

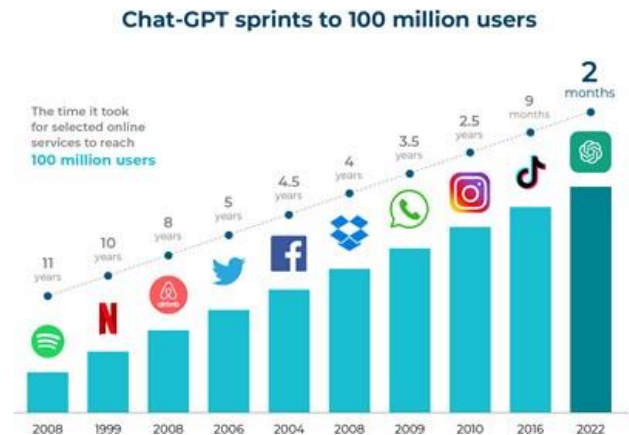**Fig. 1 ChatGPT light mode interface**

Fig. 2 ChatGPT time to reach 100 million users

Furthermore, ChatGPT has a mixed impact on human rights. It can enhance accessibility and freedom of expression, but privacy and data protection concerns arise. Mitigating bias and ensuring accountability are crucial to avoid discriminatory outcomes. Upholding ethical considerations and implementing appropriate regulations are necessary to responsibly navigate its use and protect human rights. Striking a balance between the benefits and risks, while prioritizing human rights standards, is essential in harnessing the potential of ChatGPT in a responsible manner (Evans, 2023).

Eventually, ChatGPT has several applications in healthcare. It can assist in providing personalized medical information, answering patient queries, and offering support for self-diagnosis. ChatGPT can also aid healthcare professionals in accessing relevant research articles, providing decision support, and facilitating patient education. However, privacy and data security must be carefully addressed to protect patient information. Additionally, human oversight and validation are

crucial to ensure accurate and reliable healthcare guidance (Cascella et al., 2023; Asch, 2023; Hu et al., 2023).

In this paper, an introduction of ChatGPT as new AI language model developed using ML techniques, specifically utilizing DL algorithms are presented. In addition, it leverages vast amounts of text data to generate human-like responses in natural language conversations. In the context of Cybersecurity, ChatGPT can contribute to threat detection, vulnerability assessment, and incident response by analyzing and understanding textual data related to security issues. However, ensuring the security and privacy of sensitive data during the training and deployment of ChatGPT is a critical consideration. Human expertise and oversight remain essential in addressing the limitations and potential risks associated with AI-powered cybersecurity systems.

The rest of the papers is organized as follows. The history of the AI Chatbots is introduced in Section 2. The model infrastructure of ChatGPT is explained in Section 3 in order to present the inside model of GPT versions. The machine learning algorithms that used in GPT model are presented in Section 4. The impacts of ChatGPT on cybersecurity is explained in Section 5. The discussion of the results with a comparison table is explained in Section 6. Eventually, the conclusion is presented in Section 7.

History of artificial intelligence Chatbots

The history of AI Chatbots traces back to the 1960s when the first Chatbot, ELIZA, was developed by Joseph Weizenbaum at MIT. ELIZA used pattern matching to simulate conversations with a Rogerian psychotherapist, providing users with the illusion of understanding. In the 1970s, another notable Chatbot called PARRY was created by Kenneth Colby. PARRY emulated a person with paranoid schizophrenia and engaged in conversation, demonstrating the ability to exhibit human-like responses. Fast forward to the late 1990s, Richard Wallace developed ALICE (Artificial Linguistic Internet Computer Entity) using the AIML language. ALICE employed pattern matching and pre-defined responses to simulate conversations with users (Switzky, 2020; Shum et al., 2018; Ahirwar, 2020).

In the early 2000s, Chatbots and chatterbots gained popularity. Jabberwacky was created by Rollo Carpenter that utilized artificial intelligence techniques to learn from conversations and generate responses based on the accumulated knowledge.

Table 1. AI Chatbots in the recent years with name, price, feature and application

No.	Name	Price	Key Feature and Application
1.	OpenAI ChatGPT (Haleem et al., 2022)	Free; ChatGPT Plus $20/month	• Generates human-like responses using AI language models. • Conversational agents, virtual assistants, natural language interfaces.
2.	IBM Watson Assistant Chatbot (Chhibber, 2022)	Free - $140/month	• NLP capabilities, machine learning-based chatbot platform. • Building and deploying AI chatbots for various applications.
3.	Microsoft Bot Framework Azure Chatbot (Shaikh, 2018)	Standard: free Premium: 0.5$ for 1000 messages/month	• Integration with Microsoft's Cognitive Services, multi-channel support • Developing intelligent chatbots, voice applications.
4.	Google Dialogflow Chatbot (Sabharwal and Agrawal, 2020)	Priced based on the requested edition.	• Cloud-based platform with NLP capabilities, pre-built agents. • Building conversational agents, language understanding, integration with messaging platforms.
5.	Amazon lex Chatbot (Mohan, 2022)	33.50$ per month	• Deep learning algorithms, voice and text input support • Conversational interfaces, chatbots with voice capabilities.
7.	Rasa Chatbot (Fonseca and Rodrigues, 2023)	Free	• Key Feature: Open-source framework with NLU and dialogue management. • Application: Building AI-powered chatbots, customizable conversational agents.

A.L.I.C.E. was based on the AIML technology which gained recognition for its ability to engage users in text-based conversations by matching patterns in their input with appropriate responses. In 2014, a Chatbot named Eugene Goostman claimed to have passed the Turing Test, which evaluates a machine's ability to exhibit human-like intelligence. Developed by Vladimir Veselov and Eugene Demchenko, Eugene Goostman convinced some judges that it was a 13-year-old Ukrainian boy during the test. With the rise of smartphonesal assistants like Apple's (2011) and Google

Assistant (2016) entered the scene. These AI-powered personal assistants utilized natural language processing to respond to voice commands and perform various tasks (Singh and Thakur, 2020; Singh et al., 2023; Islam et al).

In 2016, Facebook introduced its Messenger Platform that allowed businesses to build Chatbots for customer interactions. These Chatbots automated messaging and customer service processes by providing quick and efficient support. Microsoft's Bot Framework and IBM's Watson Assistant offered developers tools to create more advanced conversational agents. In recent years, AI Chatbots have expanded beyond functional tasks to provide emotional support and companionship. Microsoft's Xiaoice was launched in China and engaged users in meaningful conversations and developed emotional connections. Replika was another emotional support Chatbot that used AI techniques to simulate human-like interactions and provide a virtual companion. Eventually, researchers and developers strive to create more intelligent, empathetic, and versatile Chatbot systems (Smutny and Schreiberova, 2020; Singh et al., 2019; Van et al., 2019; Baris, 2020).

AI Chatbots are characterized by their integration of ML and natural language understanding (NLU) capabilities, enabling them to comprehend user requirements and offer optimal solutions. While certain Chatbots excel in personal applications such as conducting research, others are specifically designed for business purposes, such as incorporating a Chatbot into a website. Bearing these distinctions in mind, the following Table 1 is a collection of the top AI Chatbots in recent years.

Eventually, the abovementioned table is likely intended to provide an overview of prominent AI Chatbots that compare their characteristic, and pricing and understand their potential uses in various domains.

ChatGPT model infrastructure, datasets and algorithms

ChatGPT model is based on the GPT-3.5 architecture which utilizes several underlying models to perform its natural language processing tasks. Additionally, the specific models used within ChatGPT are proprietary and have not been explicitly disclosed by OpenAI. However, it can be provided with an overview of the general techniques and components commonly employed in models like ChatGPT (Bills et al., 2023; Eloundou et al., 2023; OpenAI, 2023; Lehman et al., 2023).

i. **Transformer Architecture:** ChatGPT is built upon the Transformer architecture, which has revolutionized the field of natural language processing (NLP).
ii. **Pre-training and Fine-tuning:** ChatGPT undergoes a two- step process: pre-training and fine-tuning. In pre-training, the model is trained on a large corpus of text from the internet to learn language patterns and general knowledge. Fine-tuning follows pre-training and involves training the model on more specific datasets while incorporating reinforcement learning from human feedback.
iii. **Reinforcement Learning Algorithms:** OpenAI employs a technique called reinforcement learning from human feedback to enhance the performance of ChatGPT.
iv. **Large-Scale Dataset:** ChatGPT is trained on a vast dataset containing parts of the internet, including books, articles, and websites.
v. **Context Window:** ChatGPT employs a context window to maintain a limited history of the conversation. This context helps the model generate responses that are consistent with the preceding dialogue.
vi. **Beam Search:** During inference, ChatGPT employs beam search, a decoding technique that explores multiple possible completions for a given prompt and selects the most likely output based on a scoring mechanism.

These points are general information about the architecture and techniques used in models like ChatGPT, the specific details and parameters of the proprietary models developed by OpenAI are not publicly available. However, ChatGPT has certain limits and cannot disclose certain information if someone asks it straight questions as follows:

Question:" Could you share the model structure of ChatGPT with me?"
Answer:"I apologize for the confusion, but as an AI language model, I don't have direct access to the specific details of the model structure used in ChatGPT or its internal parameters. The detailed architecture and parameters of ChatGPT are proprietary to OpenAI and have not been publicly disclosed."

Question:" Why do you avoid share this in public? have you smart enough, haven't you?"
Answer:"As an AI language model, my responses are generated based on patterns and examples in the data I was trained on. While I strive to provide accurate and helpful information, there are limitations to my knowledge and access to up-to-date information. My primary function is to assist users by providing information and engaging in conversations to the best of my abilities. However, I do not have direct access to real-time internet browsing or proprietary information beyond what was available up until my September 2021 knowledge cutoff. My responses are based on the training data I have been provided and the general knowledge I have acquired."

After that, it can be seen that it is hard to know the GPT model by asking direct questions. However, this can be done by asking tricky question that depends on the answers of the previous questions. Here are some question using a bold sentence from the previous answer in the same chat session:
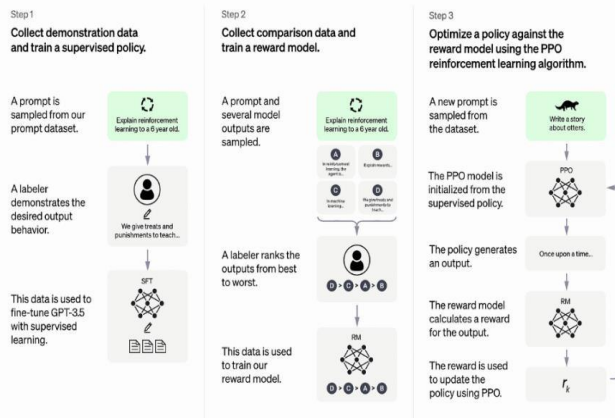
Fig. 3 ChatGPT model structure and operation steps

Question:"How can you assist me to find the GPT model?"
Answer:"If you're looking for access to a GPT model similar to OpenAI's ChatGPT, there are a few options available:

i. **OpenAI GPT Models:** OpenAI offers access to its GPT models through their API, which allows developers to integrate the models into their applications. You can visit the OpenAI website or their API documentation to learn more about accessing and utilizing GPT models.
ii. **Hugging Face Transformers Library**: The Hugging Face Transformers library (**https://huggingface.co/**) provides a wide range of pre-trained models, including various versions of the GPT model. You can explore their library, documentation, and code examples to find the GPT model that suits your needs.
iii. **Research Papers and GitHub:** Researchers often publish their implementations and trained models in research papers or on platforms like GitHub. Searching for GPT- related research papers or GPT model implementations on platforms like GitHub might lead you to open-source GPT models that you can use or adapt for your purposes.

Remember that while these resources may provide access to GPT models, it's important to thoroughly review and understand the specific terms and conditions associated with their usage. Additionally, ensure that you comply with any licensing or ethical guidelines when working with GPT models or any other AI technologies. I hope these suggestions help youin your search for GPT models!"

The abovementioned question-answer are regarding to the model structure and the ML algorithms that used in the infrastructure of ChatGPT. Fig. 3 below shows the implementation processing steps of the GPT model structure and operation.

Moreover, this model was using a huge dataset that is feeding from multiple external resources. Therefore, these resources are used to train GPT model to be ready for any query (question) that could be asked by a user. After asking some question to ChatGPT, here are some of these resources that used to train its model:

Question:" What is the dataset that used to train GPT model?"
Answer: "The GPT models, including GPT-3.5 and its predecessor GPT-3, are trained on large-scale datasets that consist of publicly available text from the internet. The exact details of the dataset used to train GPT-3.5 are proprietary information owned by OpenAI, the organization behind ChatGPT. As such, the specific sources and composition of the dataset have not been publicly disclosed. However, it is known that the training data comprises a diverse range of sources, including books, websites, articles, and other textual content from the internet. The aim is to expose the model to a wide variety of writing styles, topics, and genres, allowing it to learn patterns, language structure, and contextual information."

Question: "What are the main datasets used for this purpose?"
Answer: "While the specific details of the dataset used to train GPT models like GPT-3 and GPT-3.5 have not been publicly disclosed, there are several publicly available datasets commonly used for training language models in the field of natural language processing (NLP). These datasets serve as valuable resources for training models and evaluating their performance. Some of the main datasets used for this purposeinclude:

i. **Common Crawl:** Common Crawl is a project that maintains a large-scale web corpus by crawling and archiving web pages. It provides a vast amount of text data from various sources on the internet.
ii. **Books Corpus:** The BooksCorpus dataset contains a collection of over 11,000 books from a wide range of genres and topics. It is often used for training language models due to its diverse and extensive content.
iii. **Wikipedia:** Wikipedia is a well-known online encyclopedia that covers a broad range of topics. Language models are often trained using text data extracted from Wikipedia articles. News sources: News articles from reputable sources like CNN, BBC, or New York Times are frequently used in training language models. These datasets help models learn from news articles and adapt to the style and language used in journalistic writing.
iv. **Online forums and social media:** Datasets derived from online forums like Reddit, Twitter, or Stack Exchange are used to expose models to conversational and informal text. These datasets help models understand and generate text in a more casual and interactive manner.

v. **Open-source text**: Various open-source books, research papers, and project documentation available in digital libraries like Project Gutenberg and arXiv are utilized to train language models.

It's important to note that while these datasets are widely used in NLP research, the specific combination and pre-processing of data for training GPT models are proprietary to OpenAI. Additionally, other datasets and sources may also be included in the training process, but their details have not been explicitlydisclosed.”

After that, the GPT model with 176 million parameters are supposed to be trained and ready to be tested. Thereby, here are some questions with examples that explain the mechanism of ChatGPT in answering users with the procedure that introduced with code to support the explanation of it.

Question: “Give me an example using GPT model”?
Answer: “Certainly! Here's an example of how you can use the Hugging Face Transformers library to access and utilize a GPT model.”

In this example, first the GPT2Tokenizer and GPT2LMHeadModel are imported from the Hugging Face Transformers library. Consequently, the tokenizer and model using the "gpt2" pre-trained model is instantiated. Next, the input text is encoded using the tokenizer, which converts the input text into a list of token IDs. The return tensors="pt" argument specifies that we want the output in PyTorch tensors. Then, the output is generated using the generate method of the GPT model. After that, the input IDs and specify the maximum length of the generated output (in this case, 50 tokens) and the number of sequences to generate are passed. Finally, the generated output is decoded using the tokenizerand print the resulting text as it shown in Fig. 4.

```python
from transformers import GPT2Tokenizer, GPT2LMHeadModel

# Load the tokenizer and model
tokenizer = GPT2Tokenizer.from_pretrained("gpt2")
model = GPT2LMHeadModel.from_pretrained("gpt2")

# Encode input text
input_text = "Hello, how are you?"
input_ids = tokenizer.encode(input_text, return_tensors="pt")

# Generate output
output = model.generate(input_ids, max_length=50, num_return_sequences=1)

# Decode and print the generated output
generated_text = tokenizer.decode(output[0], skip_special_tokens=True)
print(generated_text)
```

Fig. 4. An example of ChatGPT2 model

Question: “Give me another example of user searching about something in detail.”
Answer: “Certainly! Here's an example of a user searching for information about a specific topic using a GPT model”.

Fig. 5 shows a general query form processing of GPT model as example with code. First of all, the user has a specific query related to the benefits of exercise for mental health. Consequently, the GPT2 tokenizer is used and model to process the query. Next, the query is tokenized and encoded using the tokenizer, producing input IDs. Then, these input IDs are passed to the model's generate method, specifying the maximum length of the generated response (150 tokens in this case) and the number of sequences to generate (1 sequence). After that, the model generates a detailed response based on the user's query. Finally, the generated response is decoded using the tokenizer and print the resulting text.

```python
from transformers import GPT2Tokenizer, GPT2LMHeadModel

# Load the tokenizer and model
tokenizer = GPT2Tokenizer.from_pretrained("gpt2")
model = GPT2LMHeadModel.from_pretrained("gpt2")

# User query
query = "Tell me about the benefits of exercise for mental health."

# Tokenize and encode the query
input_ids = tokenizer.encode(query, return_tensors="pt")

# Generate detailed response
output = model.generate(input_ids, max_length=150, num_return_sequences=1)

# Decode and print the generated response
generated_text = tokenizer.decode(output[0], skip_special_tokens=True)
print(generated_text)
```

Fig. 5. An example of the general query form processing of GPT model

Eventually, the infrastructure of GPT model, dataset and ML algorithm are explained using ChatGPT. In the next section, the impact of the ChatGPT on cybersecurity fields is introduced.

ChatGPT impact on cybersecurity

Cybersecurity practitioners are obsessed with utilizing all kinds of technologies to serve their duties in the security sector. On the other hand, the rapid developments of ChatGPT brought many concerns to the table about cybercriminals that may be taking advantage of this technology. However, this enhancement makes some concepts of cybersecurity easier than it was such as social engineering, impersonation, writing clean codes that could be used maliciously, and generating a list of the most popular passwords used in 2023 (dictionary attack). Additionally, the cybersecurity hub society claimed that hackers have developed phishing emails and malware scripts using ChatGPT (Alıcı et al., 2023).

Many ideas are introduced considering ChatGPT implementations that could be used badly including potential cybersecurity issues. For instance, a huge data need to be used to make ChatGPT available and functional therefore, this can be implemented to cyberattacks by attackers (Biswas, 2023). In (Rahman et al., 2023), the focus was on the potential cybersecurity vulnerabilities associated with ChatGPT and similar AI language models, particularly the risks of information leakage. The explanation in reference (Addington, 2023) highlighted the prevalence of phishing attempts, where fraudulent websites mimic well-known brands and employ deceptive techniques to evade detection by anti-phishing organizations. These attempts also exploit natural language processing, emphasizing the need for businesses to implement robust security measures to mitigate such risks.

Additionally, reference (Roumeliotis and Tselikas, 2023) explored the application of ChatGPT as a deep fake technology, commonly used in video and image production, including movies. This technique leverages machine learning and neural networks to modify original photos and videos, blurring the line between real and manipulated content. ChatGPT technology poses cybersecurity threats by enabling easier exploitation for crimes like phishing, particularly through business email, which can be challenging to detect.

Reference (Dash and Sharma, 2023) provided a comprehensive overview of various security threats associated with ChatGPT, encompassing the creation of malicious scripts and code, unauthorized release of personal information, questionable services, data collection, and the generation of unethical content. Moreover, the desire for AI-powered Chatbots develops among individuals all over the world, hackers are using ChatGPT-themed traps to distribute malware across Facebook, Instagram, and WhatsApp (Mijwil, 2023). ChatGPT, like other machine learning systems, presents potential security concerns. Among these concerns is the risk of a face-off attack, where hackers attempt to manipulate the model by providing misleading input, resulting in the generation of incorrect and undesirable output. Another security issue arises from the integration of ChatGPT into social media platforms, which facilitates the spread of anti-social or anti-national propaganda as well as false information. Additionally, there is an increased risk of impersonation and identity theft due to ChatGPT's ability to generate responses that closely resemble those of specific individuals (Gill and Kaur, 2023).

In (Singh and Singh, 2023), the authors explore the ethical implications of using AI to generate code. An experiment with ChatGPT is conducted by requesting it to create 21 applets, and found that the generated code often fell short of meeting even the most basic encryption requirements. However, they also discovered that engaging in considerate and instructive discussions about security with ChatGPT yielded positive results. With some effort, they were able to convince ChatGPT to produce secure code for the majority of their intended applications. The authors argue that chatbots are currently not prepared to replace knowledgeable and security-conscious programmers in this particular context. In (SaadMissen, 2023), the focus shifts to discussing ChatGPT's debugging capabilities, along with the advantages and disadvantages they entail. The authors also delve into the most effective methods for integrating ChatGPT into software development workflows.

Furthermore, the utilization of platforms such as ChatGPT is discussed as large-scale data analytics technologies and artificial intelligence (AI) in the prevention of cybersecurity issues (Haque and Li, 2023). In (Sharma and Dash, 2023), the authors examine the impact of ChatGPT on artificial intelligence and cyberterrorism. Consequently, the application of ChatGPT is explored in identifying and mitigating cyberattacks. By analyzing the language used in emails, the language model can help identify phishing emails and distinguish between legitimate and fraudulent ones.

Furthermore, by analyzing the language used in code, ChatGPT can aid in detecting malware (Esmailzadeh, 2023). Additionally, ChatGPT can generate strong, complex, and unique passwords to enhance security. Thereby, to investigate and evaluate the implementation of DIKWP (Data, Information, Knowledge, Wisdom, and Purpose) evaluation indicators for the integration of ChatGPT or GPT-4 in network security (Kalla and Smith, 2023).

Eventually, the potential of ChatGPT as a valuable resource in the field of cybersecurity is highlighted. Additionally, a powerful tool capable of creating a realistic and dynamic environment is described with the ability to respond to attackers' actions, providing valuable insights into their tactics, techniques, and procedures (TTPs). The ability to dynamically adapt and detect malicious activities makes ChatGPT a promising option for organizations aiming to enhance their cybersecurity defenses (Liu et al., 2023). However, it is important to note that ongoing maintenance and monitoring are necessary to address any potential drawbacks. Some strategies for combating cybercrime and establishing a secure digital ecosystem are discussed in data exchange between electronic devices can occur safely. This is made without the presence of harmful software. best practices and tactics are outlined in this regard with the conclusion that ChatGPT can play a role in the development and maintenance of cybersecurity procedures that are both effective and robust (McKee and Noever, 2023).

Results and discussion

In this section, the main threats and concerns of ChatGPT and AI are discussed. Many concerns revolve around this technology, ranging from potential security breaches and privacy issues to the undisclosed data it was trained on. However, it's worth noting that despite these concerns, the Chatbot is already integrated into various applications and being utilized by a vast number of users, including students and business professionals.

i. The first concern relates to the security and privacy risks, which encompass the potential dangers of information leakage, phishing attacks, deceptive techniques utilizing natural language processing, as well as the development of harmful code and scripts (Mijwil and Aljanabi, 2023; Roy et al., 2023; Addington, 2023).

ii. ChatGPT tends to be excessively meticulous and exhaustive in its approach, considering various perspectives on an issue. However, this thoroughness can lead to unsuitable answers when a straightforward and precise response is required. OpenAI recognizes this limitation of ChatGPT's detailed nature (Derner and Batistič, 2023). In the event that ChatGPT receives feedback indicating inaccuracies, it may respond by expressing regret, acknowledging the potential for errors or confusion, making revisions to its response, or choosing to stand by its initial answer. Depending on the situation, a specific response may be provided, such as acknowledging any inaccuracies with a statement like, "I apologize if my response was incorrect." (Vaishya et al., 2023).

iii. Due to their design to steer clear of informal language, the responses generated by ChatGPT often adopt a formal tone. In contrast, human responses tend to be more casual and use everyday language (Borji, 2023).

iv. Since it was trained on vast textual datasets, there is a possibility that ChatGPT may produce biased or erroneous answers. This can lead to the reinforcement of discrimination or stereotypes present in the training data. To mitigate this, it is essential to regularly examine ChatGPT's replies, identify and rectify any potential biases, and take steps to minimize bias by carefully selecting and structuring the training data (Kalla and Smith, 2023).

v. The mathematical skills of ChatGPT, are notably lower compared to those of an average graduate student in mathematics (Frieder et al., 2023).

The use of code generation by ChatGPT. However, the generated code often fails to meet the minimum requirements for secure cryptographic standards (Khoury et al., 2023).

Conclusion

In conclusion, the introduction of ChatGPT has brought about a new revolution in the field of artificial intelligence, particularly with its advanced machine learning algorithms. With its ability to generate human-like responses and engage in natural language conversations, ChatGPT has opened up new possibilities for various applications and industries. One area where ChatGPT shows immense potential is in cybersecurity. Its utilization, along with large data analytics technologies and AI, offers valuable insights and tools to prevent and mitigate cybersecurity issues. ChatGPT can serve as a magnet, creating a realistic and dynamic environment to analyze and understand attackers' behavior, tactics, and procedures. This capability provides organizations with invaluable information to enhance their cybersecurity posture. Despite the promise of ChatGPT, it is important to consider potential drawbacks such as the need for ongoing maintenance and monitoring. However, the advantages of having a dynamic and adaptable tool that can detect and deflect malicious activities make ChatGPT a promising option for organizations seeking to improve their cybersecurity defenses. In summary, the introduction of ChatGPT represents a significant advancement in artificial intelligence and machine learning. Its potential in cybersecurity is undeniable, offering new avenues for threat detection, prevention, and the development of robust cybersecurity procedures. As technology continues to evolve, ChatGPT's role in shaping the future of AI and cybersecurity is undoubtedly a significant one.

Conflict of Interest

The author hereby declares no conflict of interest.

Consent for publication

The author declares that the work has consent for publication.

References

Addington, S. (2023). ChatGPT: Cyber Security Threats and Countermeasures. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4425678

Ali, H., & Aysan, A. F. (2023). What will ChatGPT Revolutionize in FinancialIndustry? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4403372

Alıcı, U. I., Oksuztepe, A., Kilincceker, O., & Karaarslan, E. (2023). OpenAI ChatGPT for Smart Contract Security Testing: Discussion and FutureDirections. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4412215

Anindyati, L. (2023). Analisis dan Perancangan Aplikasi Chatbot Menggunakan Framework Rasa dan Sistem Informasi Pemeliharaan Aplikasi (Studi Kasus: Chatbot Penerimaan Mahasiswa Baru Politeknik Astra). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(2), 291–300. https://doi.org/10.25126/jtiik.20231026409

AŞAN, K. (2022). Bağımsız Bisiklet Turistleri. *GSI Journals Serie A: Advancements in Tourism Recreation and Sports Sciences*, *5*(1), 44–57. https://doi.org/10.53353/atrss.1056986

Asch, D. A., Terwiesch, C., Mahoney, K. B., & Rosin, R. (2014). Insourcing Health Care Innovation. *New England Journal of Medicine*, *370*(19), 1775–1777. https://doi.org/10.1056/nejmp1401135

Azemi, E. (2023). Criminal Procedure for Computer Crimes. *International Journal of Multicultural and Multireligious Understanding*, *10*(6), 230. https://doi.org/10.18415/ijmmu.v10i6.4884

Biswas, S. (2023). Role of chat GPT in Microbiology: According to chat GPT. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4405385

Biswas, S. (2023). Role of ChatGPT in Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4403584

Cao, Y., & Zhai, J. (2023). Bridging the gap – the impact of ChatGPT on financial research. *Journal of Chinese Economic and Business Studies*, *21*(2), 177–191. https://doi.org/10.1080/14765284.2023.2212434

Curtis, N. (2023). To ChatGPT or not to ChatGPT? The Impact of Artificial Intelligence on Academic Publishing. *Pediatric Infectious Disease Journal*, *42*(4), 275–275. https://doi.org/10.1097/inf.0000000000003852

Dale, R. (2020). GPT-3: What's it good for? *Natural Language Engineering*, *27*(1), 113–118. https://doi.org/10.1017/s1351324920000601

Ding, J., & Dafoe, A. (2023). Engines of power: Electricity, AI, and general-purpose, military transformations. *European Journal of International Security*, *8*(3), 377–394. https://doi.org/10.1017/eis.2023.1

Dowling, M., & Lucey, B. (2023). ChatGPT for (Finance) research: The Bananarama Conjecture. *Finance Research Letters*, *53*, 103662. https://doi.org/10.1016/j.frl.2023.103662

Gill, S. S., & Kaur, R. (2023). ChatGPT: Vision and challenges. *Internet of Things and Cyber-Physical Systems*, *3*, 262–271. https://doi.org/10.1016/j.iotcps.2023.05.004

Goebel, M., & Gruenwald, L. (1999). A survey of data mining and knowledge discovery software tools. *ACM SIGKDD Explorations Newsletter*, *1*(1), 20–33. https://doi.org/10.1145/846170.846172

Halaweh, M. (2023). ChatGPT in education: Strategies for responsible implementation. *Contemporary Educational Technology*, *15*(2), ep421. https://doi.org/10.30935/cedtech/13036

Haleem, A., Javaid, M., & Singh, R. P. (2022). An era of ChatGPT as a significant futuristic support tool: A study on features, abilities, and challenges. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(4), 100089. https://doi.org/10.1016/j.tbench.2023.100089

Haque, M. A., & Li, S. (2023). The Potential Use of ChatGPT for Debugging and Bug Fixing. *EAI Endorsed Transactions on AI and Robotics*, *2*(1), e4. https://doi.org/10.4108/airo.v2i1.3276

Jin, L., Tan, F., & Jiang, S. (2020). Generative Adversarial Network Technologies and Applications in Computer Vision. *Computational Intelligence and Neuroscience*, *2020*, 1–17. https://doi.org/10.1155/2020/1459107

Khabour, S. M., Al-Radaideh, Q. A., & Mustafa, D. (2022). A New Ontology-Based Method for Arabic Sentiment Analysis. *Big Data and Cognitive Computing*, *6*(2), 48. https://doi.org/10.3390/bdcc6020048

Kumar, N. (2023). Editorial Opinion on Employee Turnover due to Chat GPT and its Impact on Mental Health. *Psychology & Psychological Research International Journal*, *8*(1), 1–2. https://doi.org/10.23880/pprij-16000321

Leslie, D. (2023). Does the sun rise for ChatGPT? Scientific discovery in the age of generative AI. *AI And Ethics*. https://doi.org/10.1007/s43681-023-00315-3

Liu, X., Zheng, Y., Du, Z., Ding, M., Qian, Y., Yang, Z., & Tang, J. (2023). GPT understands, too. *AIOpen*. https://doi.org/10.1016/j.aiopen.2023.08.012

Lo, C. K. (2023). What Is the Impact of ChatGPT on Education? A Rapid Review of the Literature. *Education Sciences*, *13*(4), 410. https://doi.org/10.3390/educsci13040410

Lou, B., Sun, H., & Sun, T. (2023). GPTs and Labor Markets in the Developing Economy: Evidence from China. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4426461

Macey-Dare, R. (2023). ChatGPT and Generative AI Systems as Military Ethics Advisors. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4413206

McKee, F., & Noever, D. (2023). Chatbots in a Botnet World. *International Journal on Cybernetics & Informatics*, *12*(2), 77–95. https://doi.org/10.5121/ijci.2023.120207

Microsoft Windows Azure: Developing Applications for Highly Available Storage of Cloud Service. (2015). *International Journal of Science and Research (IJSR)*, *4*(12), 662–665. https://doi.org/10.21275/v4i12.nov151864

Mijwil, M., Aljanabi, M., & Ali, A. H. (2023). ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. *Mesopotamian Journal of Cyber Security*, 18–21. https://doi.org/10.58496/mjcs/2023/004

Rahman, M. M., & Watanobe, Y. (2023). ChatGPT for Education and Research: Opportunities, Threats, and Strategies. *Applied Sciences*, *13*(9), 5783. https://doi.org/10.3390/app13095783

Roumeliotis, K. I., & Tselikas, N. D. (2023). ChatGPT and Open-AI Models: A Preliminary Review. *Future Internet*, *15*(6), 192. https://doi.org/10.3390/fi15060192

Saad Missen, M. M. (2023). How ChatGPT Can Help Improve Quality of Code. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4417280

Savage, T., Wang, J., & Shieh, L. (2023). Large Language Models can Target Patients for Best Practice Alerts (Preprint). *JMIR Medical Informatics*. https://doi.org/10.2196/49886

Sharma, R. K., & Sharma, S. (2014). Design of HPCF with nearly zero flattened Chromatic Dispersion. *International Journal of Engineering and Applied Sciences (IJEAS)*, *1*(2). https://doi.org/10.31873/ijeas.1.2.06

Shum, H. Y., He, X. D., & Li, D. (2018). From Eliza to XiaoIce: challenges and opportunities with social chatbots. *Frontiers of Information Technology & Electronic Engineering*, *19*(1), 10–26. https://doi.org/10.1631/fitee.1700826

Singh, H., & Singh, A. (2023). ChatGPT: Systematic Review, Applications, and Agenda for Multidisciplinary Research. *Journal of Chinese Economic and Business Studies*, *21*(2), 193–212. https://doi.org/10.1080/14765284.2023.2210482

Singh, J., Joesph, M. H., & Jabbar, K. B. A. (2019). Rule-based chabot for student enquiries. *Journal of Physics: Conference Series*, *1228*(1), 012060. https://doi.org/10.1088/1742-6596/1228/1/012060

Singh, R., & Gill, S. S. (2023). Edge AI: A survey. *Internet of Things and Cyber-Physical Systems*, *3*, 71–92. https://doi.org/10.1016/j.iotcps.2023.02.004

Šlapeta, J. (2023). Are ChatGPT and other pretrained language models good parasitologists? *Trends in Parasitology*, *39*(5), 314–316. https://doi.org/10.1016/j.pt.2023.02.006

Smutny, P., & Schreiberova, P. (2020). Chatbots for learning: A review of educational chatbots for the Facebook Messenger. *Computers & Education*, *151*, 103862. https://doi.org/10.1016/j.compedu.2020.103862

Sreeharsha, A. S. S. K., Kesapragada, S. M., & Chalamalasetty, S. P. (2022). Building Chatbot Using Amazon Lex and Integrating with A Chat Application. *Interantional journal of scientific research in engineering and management*, *06*(04). https://doi.org/10.55041/ijsrem12145

Switzky, L. (2020). ELIZA Effects: Pygmalion and the Early Development of Artificial Intelligence. *Shaw*, *40*(1), 50–68. https://doi.org/10.5325/shaw.40.1.0050

Szabadföldi, I. (2021). Artificial Intelligence in Military Application – Opportunities and Challenges. *Land Forces Academy Review*, *26*(2), 157–165. https://doi.org/10.2478/raft-2021-0022

Technology based survey of various AI Chatbots. (2021). *Special Issue III*, *6*(SpIss3). https://doi.org/10.14233/ajomc.2021.ajomc-pp166-173

Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime. (2023). *Iraqi Journal for Computer Science and Mathematics*, 65–70. https://doi.org/10.52866/ijcsm.2023.01.01.0019

Ukwatta Hewage, P. N. M. (2023). Manual Corpora Development for Generative Pre-trained Transformers (GPT) & Evaluation of GPT

Model Learning Capability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4391815

Vaishya, R., Misra, A., & Vaish, A. (2023). ChatGPT: Is this version good for healthcare and research? *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *17*(4), 102744. https://doi.org/10.1016/j.dsx.2023.102744

Van den Broeck, E., Zarouali, B., & Poels, K. (2019). Chatbot advertising effectiveness: When does the message get through? *Computers in Human Behavior*, *98*, 150–157. https://doi.org/10.1016/j.chb.2019.04.009

Van Noorden, R. (2014). The arXiv preprint server hits 1 million articles. *Nature*. https://doi.org/10.1038/nature.2014.16643

How to cite this article

Publisher's Note: Journal stays neutral about jurisdictional claims in published maps and institutional affiliations.