Research into LLM (Chat Bot) AI

Harrison Watycha

Summary

This report will discuss the research found on LLM (Chat Bot) AI, with the purpose of establishing enough information as possible about Large Learning Model in relation to AI (chat bot). I will use peer reviewed sources and academic sources to generate as much information as possible. From this we will then evaluate what LLM chat bot is the strongest and most effective. Additionally, this report will also explore the possible implementation steps of introducing an LLM (chat bot) AI into a possible system.

Introduction

Background

When discussing the rise of LLM chat bot, it is such an expansive space that is constantly evolving. As discussed by the source of Sachdeva (2024, pg.148), the LLM (chat bot AI) has grown in capability over the last five years due to multiple reasons. The first being, an increase in computing power and hardware, which allows for more complex work like creation of LLM and chat bots. Additionally, the source Rolf Fredheim (2024, pg.14) in his academic journal proposes that the algorithms and infrastructures now available to programmers have opened the opportunity for an increase in chat bot's. This proposal from Fredheim, has explained how chat bots utilise powers to read and analyse the user's request before searching the databased to provide a sensible and relevant answer. The structure of an LLM includes multiple neutral language models, and a deep learning algorithm. This enables the AI to recognise and provide outputs for the user inputs.

Purpose of the Research

There is significant amount of research and reporting into LLM chat bot AI which makes it easy to research the capability of LLM. This research that has been conducted into LLM has constantly highlighted the strength of GPT which has been created by Chat AI. GPT has numerous versions of the chat bot, either the 3.5 or 4.0 version. The purpose of this research is to gain a deeper insight into the LLM (chat bot) it's capabilities and the possible implementation. This research to complete its purpose will utilise case studies and examples to gather as much information as possible. This research will also indicate possible costs and benefits of implementing an LLM chat bot, to indicate some forecasting for anyone looking to implement the process.

Role of AI (chat bot) in Cybersecurity

AI is heavily progressing and enhancing cybersecurity as a collective from the attackers point of view of from people implementing cybersecurity measures. Best described in the source of Lin (2024, pg.120) stating that AI has created new powers and new capabilities and if for the user at the touch of button. Whilst this is a simple sentence, it does bear a lot of merit since AI does now provide attackers will ideas and possible code and access routes that could become harmful. However, it does go both ways as the source of Lin (2024, pg.121) explores how chat bot provides coding and technical knowledge to create infrastructure and frameworks to defend data from attackers all provided through chat bot.

Case Studies/ Examples of Successful Use Cases

Case Study 1: GPT

- GPT was released in 2018, and it has been described as one of the most effective chat box's. It heavily focuses on being a user focused chatbox by allowing the user to steer and control the conversation.
- It heavily utilises statistics and probabilities from the user to articulate its response. Per Lin (2024, pg.18), it understands language due to it being a LLM and then will generative a response based on the probability of what is being asked
- The result and effectiveness has been scored by percentage. Depending on the exact model, it ranges from 68 percent and 84 percent accurate. This does make GPT quite the accurate chat box.
- The advantages of using a chat box and include:
- Being cost effective, it provides a response extremely effectively and will not leave the user waiting. It also provides an accurate source of information to an extent.
- However, the disadvantages do include:
- It is not 100 percent accurate and can make mistakes. Also, the chat box can be restricted in its responses meaning that it cannot answer every single possible question.

Case Study 2: Claude

- Claude is an effective LLM chat bot, in comparison to GPT it can consume large documents, and is more suited to reading and processing large files and documents.
- The steps to implement to Claude include paying for the service, this chat bot is free to an extent. You do have to create an account and join Anthropic API. From that you will be granted an API which will finish the installation process.
- In terms of how effective Claude it is explored to be approximately 60 percent accurate. Whilst lower, it is made clear by numerous sources that is accurate for a large files and documents.
- Challenges faced and solutions implemented with Claude has included the challenge fairness and being un-bias. Creating a chat bot that pulls information without having any form of biasness as the AI will process data that may have implemented biasness. Also, it is clear that with most AI systems there are some privacy concerns around the use of the data provided and ensuring the chat bots are all following the supported regulations. A disadvantage of Claude, does include the fact it is not the most effective responsive to message chat bot unlike GPT.

Discussion

Key Findings

The key findings that have been learnt in this report include that different chat bots excel in different roles and have different purposes. It has also been made clear that they cannot understand extremely complex questions, slang and have a lack of understanding. Additionally, an advantage of these chat bots using AI is that the provide effective sources and solutions to problems the asking user may have. Furthermore, another key finding of the LLM chat bot's is that they are all very versatile meaning they can be integrated efficiently and they can support multiple languages (coding, natural languages etc).

Best Practices and possible implementation

The best form of implementation and practices to ensure is firstly design and defining the objectives and making sure it is centred around accessibility for the user. Following this, a good practice for implementation is to develop and develop the LLM by starting simple and making sure data privacy is a principle of the foundation to support the users. Final overall step is to ensure you monitor to your LLM for any bugs or flaws and ways to implement any increase of capabilities. By following this very broad overall plan, specific steps are important but this will ensure you are practicing effectively.

Challenges and Solutions

The challenges faced by practicing chat bot and implementing this form of AI, is firstly it can be significantly technical to implement and you will need to dedicate a large amount of time to ensuring everything is to an effective standard. Following that, this research has shown that it is also a resource challenge of having the required and skilled personnel working on the steps and being able to fund that work and project. Additionally, a challenge in any LLM chat bot is making sure you adhere to a legal considerations and ethics as if you do not follow this, there will be legal consequences or you will find consumers do not want you support your system and ultimately your product.

Conclusion and Prototype Layout

Summary of Key Points

From the research the key points that have been highlighted are the process and accuracy of these LLM's, they run a lot of data collection and can be highly accurate with their output.

Additionally, they have been shown to be not be 100 percent and can make mistakes that the user may take as the truth.

Furthermore, they can also have a sense of biasness based on the material provided to them and what they consume, this too can be passed on to the user.

Finally, the process of the implementation can be lengthy and complex, however if you follow the correct steps of data collection, feature engineering, model and tokenization and make sure the output is correct you will find an effective LLM.

Prototype Layout and outcome

With the research and case study explored it has become clear that we should utilise BERT and GPT-4. This way we have an effective model that will handle most tasks, complex or not. It will provide a high level of performance and will also have strong capabilities in retrieval. The layout would need specific NLP language with a user interface (UI), whilst also and including the background infrastructure that would have to include cloud hosting and implementation of API'S. Furthermore, the key feature in implementing would be installing data encryption, and access control to prevent any unauthorised user's from gaining access to the storage of the user's data and going on to exploit that. Coinciding with that would be ensuring the LLM chat bot is not influenced by any form of biasness and being transparent about the data collection, and ultimately the usage of the data supplied by the user's. Finally, combing Claude's document file size capabilities and GPT's higher accuracy, it makes for a very effective prototype. So, in conclusion, this report has displayed a potential open source model would make GPT or Claude an effective choice or if in creating your own LLM you could combine the certain discussed features and implement those features.

References

- Fredheim, R. (2024). Assessing the risks and opportunities posed by AI-enhanced influence operations on social media. *Place Branding and Public Diplomacy*. doi:https://doi.org/10.1057/s41254-023-00322-5.

- Sachdeva, A. (2024). Taking the Chat out of Chatbot? Collecting User Reviews with Chatbots and Web Forms. *Journal of Management Information Systems*, 41(1), pp.146–177. doi:https://doi.org/10.1080/07421222.2023.2301175.

- Lin, J. (2024). How Can I Get It Right? Using GPT to Rephrase Incorrect Trainee Responses. *International Journal of Artificial Intelligence in Education*. doi:https://doi.org/10.1007/s40593-024-00408-y.