1 Background

The objective of this initiative is to enhance the effectiveness of the search function on websites, with a particular focus on enhancing the performance of the input box. As outlined in [**?**] , 69% of users initiate a search for products directly via the search bar. However, 80% of these users subsequently depart from the webpage due to unsatisfactory experiences with the search functionality. In this study, 41% of respondents expressed frustration regarding the display of irrelevant content. A further issue that was identified as a point of frustration for 32% of users was the presentation of products that were no longer available. A further issue that 26% of users encounter with contemporary search systems on websites is the inability of these systems to accurately interpret user queries. To illustrate, when one seeks to procure a dresser and inaccurately enters "closet" as the search term, the websites encounter difficulties in locating the desired item.

A total of 69% of users have confirmed that they encounter irrelevant search results, and of those, 35% have indicated that this behavior prompts them to leave the webpage. A further 27% of users have confirmed that they have abandoned webpages due to the inability to restrict their searches. An additional 26% have done so due to out-of-stock status. A further notable issue is the absence of error tolerance in current websites, which results in the failure to display outcomes in instances of typographical inaccuracy.

1.1 Translation difficulties between text and SQL(A)

Achieving an accurate interpretation of the user's intent in the context of translating text into SQL poses a considerable challenge. This is due to the fact that some words could be ambiguous or the user might use synonyms. The system should also demonstrate fault-tolerance capabilities, as it is expected to generate a query in the event of typing errors. As previously stated in [**?**], it is imperative to exercise caution to ensure that the system does not generate erroneous queries. Otherwise, there is a risk of diminishing user trust in the website. As elaborated upon in [**?**], users demonstrate a reluctance to trade a user interface that is characterised by reliability and predictability for an intelligent system that is deemed unreliable.

1.2 Privacy concerns(A)

Furthermore, it must be considered that non-technical users can also exploit the system by requesting private data. This scenario poses significant privacy concerns, given that the users can bypass any need to understand SQL, and instead simply request the data they desire from the LLM. In such systems, the implementation of measures designed to restrict access to data is essential for ensuring the security of private data. According to the Open Worldwide Application Security Project (OWASP), which is a non-profit organization that aims to improve the security of software projects, SQL-Injections are still in the Top 10 Security Risks of 2021 and it is likely that they will remain in the Top 10 of 2025, taking into account that they were the number one attack in the Top 10 of 2017 [**?**].

1.3 Problem with existing text-to-sql(A)

The rule-based method for generating SQL queries was presented in the paper [**?**]. However, several issues were identified in the course of this approach, which were addressed to a limited extent. As previously mentioned, the system is confronted with ambiguous words. In [**?**], the recommendation was made to present the user with all possible variants that can be derived from the multi-word term. This enables the user to make an informed decision, ensuring an appropriate interpretation of their intention. A further challenge arises when a word is not present in the lexicon,

as no query is generated in this instance. In such a scenario, it is imperative for the user to reformulate their query in a manner that is comprehensible to the system. However, this approach introduces a significant disadvantage, as the preliminary query may be processed by the system, but its execution is precluded due to the system's limited capabilities. The maintenance of synonyms poses a considerable challenge, as it is necessary to provide potential users with the opportunity to consult them. Consequently, a continuous adaptation of the system is required to ensure the quality of the results of the searches. As demonstrated in [**?**], a further issue is the considerable duration of user inquiry processing. In this study, a processing duration of six seconds was observed, which is regarded as relatively extensive when compared to the duration of a search in a web-based store. Nonetheless, a pivotal element was absent from the previously mentioned papers: the context of the values stored in the database. To illustrate, supplementary information becomes pertinent when storing the age of dogs. This necessity arises from the potential for storing the age of dogs in either months or years. Depending on the specific context, additional rules may be in place that must be taken into consideration.

Text-to-SQL systems that leverage LLMs have been developed; a notable example is SQLAI.AI [1]. Despite its development for developers, SQLAI.AI is not suitable for practical application.

[1] https://www.sqlai.ai/