Translating text to SQL-Queries ensuring a privacy preserving AI

Bergische Universität Wuppertal

THIVYAN SIVANANTHAN, JACOB ORTENBERG, and PARSSA JASHNIEH

Typically, when a user interacts with a website, such as searching for an item or filtering the search results, a SQL template is used for which the user input gets added. By using an AI that translates natural language into SQL queries, the initial search results based on the keywords passed will most likely be tailored to the user's wishes, providing better search results initially without the need to interact with filters. To ensure regulatory compliance, such as not being able to use passwords as a search criterion, we assert a privacy preserving AI that can easily be integrated into an existing code/database.

CCS Concepts: • **Human-centered computing** → *Web-based interaction*; Interaction design theory, concepts and paradigms.

Additional Key Words and Phrases: AI, Seq2Seq, SQL, UI, UX, Filters, Search, Transfer Learning, NLP

ACM Reference Format:

Thivyan Sivananthan, Jacob Ortenberg, and Parssa Jashnieh. 2025. Translating text to SQL-Queries ensuring a privacy preserving AI. In *Final Project for the HIC Module at the Bergische Universität Wuppertal(Human-Computer Interaction & Artificial Intelligence), October 7–February 28, 2025, Wuppertal, Germany*. ACM, Wuppertal, North Rhine Westphalia, Germany, 9 pages.

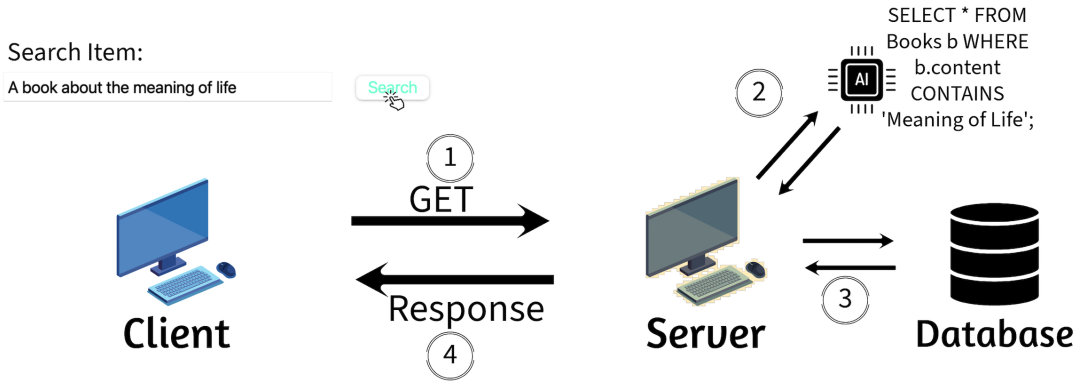

Fig. 1. Highlighting the interaction paradigm of the user with an AI. Instead of traditionally passing the users input to a static SQL-Template, it is passed to an AI-System that interpretes the users search request and dynamically generates a SQL-Query . The resulting query is then executed and displayed for the user in the Interface.

Authors' Contact Information: Thivyan Sivananthan; Jacob Ortenberg; Parssa JashniehBergische Universität Wuppertal.

Manuscript submitted to ACM

1 Introduction

Online shopping platforms like Amazon and eBay have become the go-to sources for a vast range of products. However, users often face difficulties when searching for specific items, especially products with more complex or technical specifications, such as electronic devices, computer components, or specialized tools. These challenges can lead to frustration and even cause users to switch platforms in search of a better experience. The root of these difficulties lies in the individuality of search behavior, which varies between users. Some rely on generic search terms, such as "laptop," while others prefer highly specific queries, like "Dell XPS 15 9530 with Intel Core i7 and 32GB RAM." Our study found that search behavior is roughly evenly divided between these two approaches, making it essential for e-commerce platforms to optimize their search functionalities to accommodate diverse user needs. At the same time, this presents a challenge, as creating a platform that satisfies all users equally is difficult. In addition to search queries, filtering options play a crucial role in the online shopping experience. Filters help users refine their results based on criteria such as price, size, brand, technical specifications, or customer ratings. However, ineffective or overly complex filtering systems can hinder rather than enhance the search process. If filters do not align with user expectations, are difficult to use, or fail to narrow down results efficiently, users may become frustrated and abandon their search. Therefore, improving search functionalities is essential to enhance user experience, increase customer satisfaction, and ensure platform loyalty.Building upon these challenges, we propose an alternative approach to traditional search mechanisms. Instead of relying on predefined SQL templates, we suggest dynamically generating SQL queries using machine learning techniques. By leveraging AI to generate queries in real time, the system can automatically interpret the user's intent based on their input, providing more precise and relevant search results initially. If the AI performs at a high level, this approach could eventually eliminate the need for manual filtering mechanisms, as the AI would inherently incorporate these preferences into the generated query. This shift could significantly enhance human-computer interaction, making the search process more intuitive, efficient, and user-centric. To determine whether such a scenario is truly possible and to understand how users would interact with this approach, we conducted a study. To carry out this study, we implemented a prototype interface to evaluate user behavior and gather insights on the effectiveness of dynamically generated queries in direct comparison to traditional static templates.

1.1 old

In order for a user to interact with a website, an interactive element such as an input text is typically provided. Many of these input text-elements work by having a predefined SQL-Query-Template, for which the users input gets concatenated. This query then gets passed to the Database-Management-System (DBMS), which executes it and returns the result. Although this approach seems simple at first, it has some pitfalls which need to be addressed, as it is prone to attacks like SQL-Injections. 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 [2].

1.2 Generating SQL-Queries dynamically

Instead of relying on predefined SQL-Templates, we would like to propose the idea of generating SQL-Queries dynamically using Machine-Learning-Techniques.

By generating SQL-Queries dynamically, the users wishes provided in the input text can be taken into account by the

AI automatically, providing more specific search results initially. Given that the AI performs well enough, this could lead to future websites dropping filtering mechanisms entirely, such as filtering by specific brands or other features, as the AI would reflect the users wishes automatically in the generated Query, further enhancing the Human-Computer Interaction. This new kind of interaction is highlighted in Fig. 1.

1.3 Why a privacy-preserving AI is necessary

Although the idea of generating SQL-Queries automatically sounds intriguing, there are some practical challenges that have to be taken into account, when deploying the AI into a software project. Under the assumption that the AI performs well and that it is unrestrained, nothing would prevent the user from requesting search results from the AI, that contain confidential information like passwords, email-addresses or other criteria, which poses a similar threat that are resembled by SQL-Injections. Arguably, this would make the threat of SQL like Injections even worse, as users with no technical background are now able to query for confidential data as well. To mitigate that issue, we enforce a privacy-preserving AI, with the goal to never output SQL-queries that could disclose confidential data.

1.4 Gathering Data

TODO

2 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 [3] , 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.

2.1 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 [1], 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 [1], users demonstrate a reluctance to trade a user interface that is characterised by reliability and predictability for an intelligent system that is deemed unreliable.

2.2 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 [2].

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

The rule-based method for generating SQL queries was presented in the paper [1]. 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 [1], 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 [1], 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.

3 Methods

A user study was conducted to address the following research questions:

- RQ1:What characterizes typical natural language user queries to SQL systems?
- RQ2:What are the factors that influence the mismatch between user intent and displayed search results?
- RQ3:How do users prefer to fix SQL queries when they don't match their intentions?
- RQ4:What are effective ways to communicate system limitations and capabilities to users?
- RQ5:What mechanisms most influence user satisfaction with search results?
- RQ6:What are the potential drawbacks of deploying such a system in a real-world environment?
- RQ7:How necessary are filters when an intelligent system is involved?

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

The optimization of SQL queries can be achieved through various methods. One such approach entails enhancing the initial query. However, this approach may present a challenge, as it requires that the user comprehend the erroneous interpretation of the query. To optimize the request, it is first necessary to develop a more profound comprehension of the underlying system. In this regard, the method for enhancing the user experience proposed in [1] may be applicable. This method enables the user to select from among various options (RQ3).

One of the objectives of the present study is to ascertain whether users find conventional search results satisfactory or whether they perceive the system with artificial intelligence as more advantageous. We hypothesize that users will evaluate the system employing artificial intelligence more effectively than they would a conventional system. The reason for this is that users will have more ease of use when filtering content, as opposed to the more difficult experience they face when using a conventional system(RQ5).

The hypothesis that was formulated posits that filters are only required when the system fails to comprehend the user's intention. It is hypothesized that both procedures will be utilized, as the prevailing Webshop practice involves the employment of filters, which is likely to be reflected in the user study (RQ7).

3.1 Participants

In the course of the user study, a group of 13 subjects was examined. The subjects included 12 males and one female. The majority of the subjects are currently enrolled in a Bachelor's or Master's program in Informatics. The majority of the subjects had prior experience with artificial intelligence. The subjects were aware of the objective of the study, which was to evaluate the performance of the AI system in comparison to conventional systems. The objective of the present study was to ascertain whether the artificial intelligence (AI) system is capable of producing superior results in the context of searching for products.

4 Result

4.1 Good ways to fix query (RSQ3)

A significant challenge arises from the lack of transparency in artificial intelligence systems, particularly regarding the underlying processes and algorithms that generate results. Therefore, we surveyed the participants to ascertain how they would prefer to be assisted in the event that their preliminary search query did not align with their actual needs. The proponents advanced a number of intriguing concepts. For instance, the potential exists for the artificial intelligence to adjust the filters based on the user's search history. As illustrated in Figure 2, the potential appearance of the phenomenon is demonstrated. In this instance, the filter is dynamically adjusted. Therefore, the user is able to ascertain which filters the KI utilizes and, consequently, identify the potential origin of an error. Therefore, the user has the option of either utilizing the filter to resolve the issue or adjusting the initial search query.

A further potential avenue for enhancing the efficacy of the user's outcomes is the implementation of an artificial intelligence system that can evaluate the combinability of diverse features during the user's input phase. In such a case, it is essential that the user be alerted to this possibility. As demonstrated in Figure 3, the initial state is displayed, denoting the current state of affairs.The subsequent version has been enhanced to alert the user to the absence of products for a given combination of features. In this instance, the "under 2 months" feature is distinctly emphasized, as it does not result in any products. Therefore, the user has the capacity to modify the preliminary search query and discern the elements that are not compatible. The integration of this concept with the search function can result in the automatic generation of suggestions for relevant features. This concept is further illustrated in Figure 3.

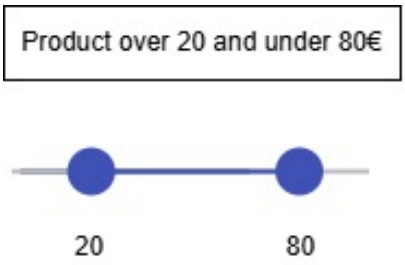

Fig. 2. AI dynamically adjusts the filters

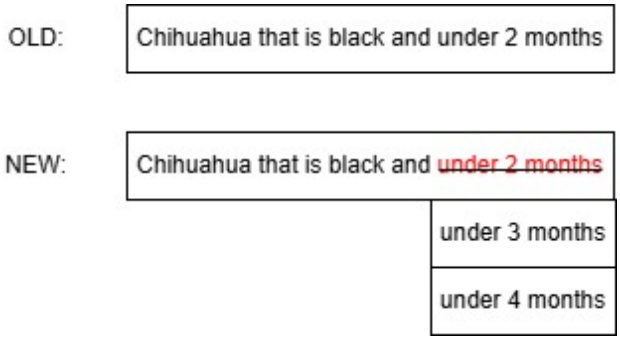

Fig. 3. AI provides information on features that cannot be combined

A further point to be considered is the potential for the AI to present analogous products in the event that the search yields minimal results. A relevant example would be a search for dogs that are of medium size. In the event that the available results are limited, the artificial intelligence could be programmed to display dogs of smaller stature.

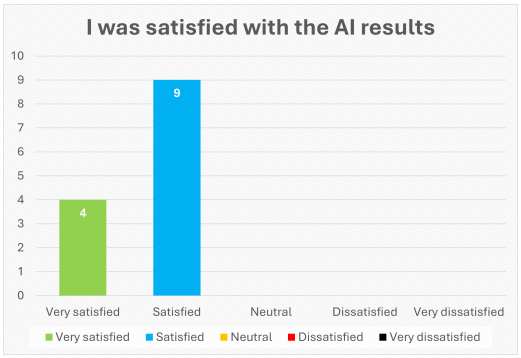

Fig. 4. AI dynamically adjusts the filters

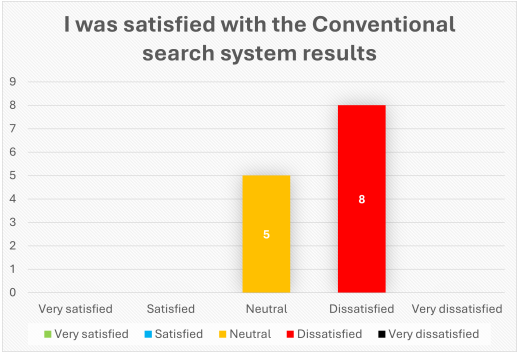

Fig. 5. AI provides information on features that cannot be combined

4.2 User Satisfaction (RSQ5)

A further aspect that was examined in our user study was the extent to which users expressed satisfaction with the outcomes produced by both the AI and conventional systems.

As illustrated in Figure 4, all participants who contributed to the study expressed satisfaction with the outcomes generated by the AI. A considerable proportion of the users, amounting to 30%, expressed profound satisfaction with the outcomes, attributing this positive sentiment to the effective comprehension of their intentions by the artificial intelligence system.

A review of the satisfaction levels observed in conventional systems clearly indicates a preference for AI, as demonstrated in Figure 5. However, it should be noted that the study revealed a notable observation: the presence of a decline in the utilization of filters by users, coinciding with the enhanced comprehension of user intentions by the AI system. This phenomenon led to the suboptimal performance of the conventional system in comparison to the AI-based

alternative. Therefore, it is important to consider the potential for a filter bias. Therefore, the users' discontent with the results is understandable. It is possible that the results would have been more favorable had the experiment been conducted differently.

4.3 Importance of Filters (RSQ7)

One of the objectives of the user study was to ascertain the importance of filters for users in the context of search results. This was particularly relevant in scenarios where the efficacy of search engine algorithms in generating relevant results is already well-established.

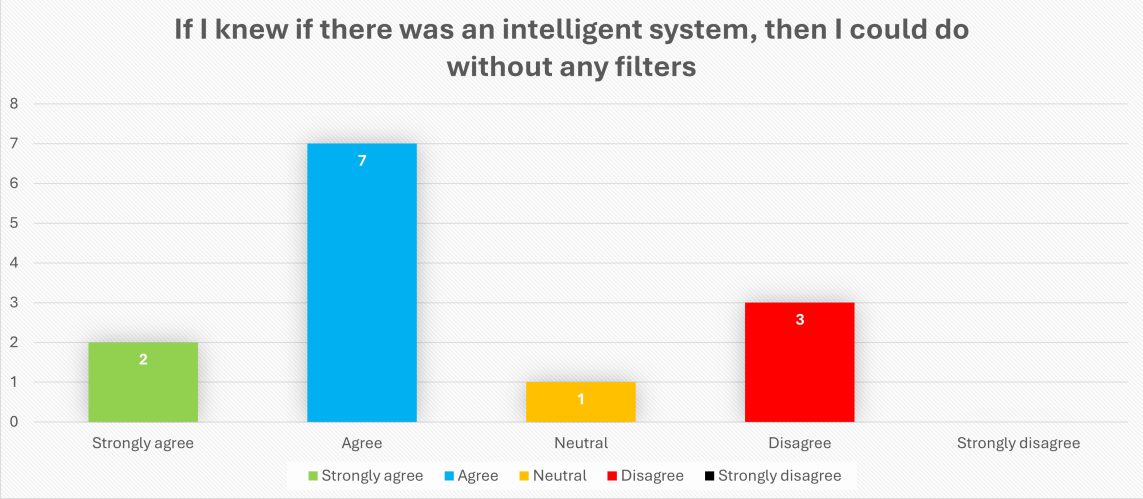

Fig. 6. AI provides information on features that cannot be combined

As illustrated in Figure 6 , there is considerable variation in opinion among the users. Approximately 70% of users affirm that, should such a system be in place, the absence of filters would be acceptable to them. Nonetheless, approximately 20% of respondents indicated a preference for maintaining web filters, even in the context of a system that incorporates these filters. The underlying reason for this phenomenon is that users prefer to utilize visual filters, such as sorting or price filters, rather than using it through tipping. The proponents indicated that the process of establishing the price filter is straightforward. They noted that this is due to the ability to swiftly determine the range of products in question, as opposed to the more cumbersome method of manual calculation. Five of the propants who expressed agreement also indicated a desire for additional practical filters, like the previously mentioned filters, such as price and sorting. This additional desire for filters is the reason why they did not strongly agree. Therefore, even if a system with AI is used, it is important to maintain filters.

5 Discussion

The objective of the paper is to propose the development of an artificial intelligence (AI) system designed to facilitate the search process for products by users.

5.1 Use of Filter

The user study revealed that the majority of users preferred to work with the filters first. This phenomenon may be attributed to the fact that contemporary systems are generally designed to assume that users will employ search filters during the search process. Consequently, users may find it unconventional to utilize solely the search bar to perform a search. The utilization of artificial intelligence by the majority of users does not align with conventional practices, as individuals have become accustomed to employing filters within online shopping platforms rather than utilizing the capabilities of AI directly. Following a series of inquiries, a conclusion was reached: The users have adapted to the system and are now able to discern whether the AI comprehends their intentions. Consequently, the majority of users have increasingly relied on the AI rather than the filters. Therefore, a period of adaptation is required for users to acclimatize to the KI. It is imperative to acknowledge the pivotal role of artificial intelligence in the integration of such systems within e-commerce platforms. The objective is to cultivate a conscious awareness among users.

5.2 Improvement through AI

The implementation of artificial intelligence has yielded notable enhancements in the realm of product search, thereby facilitating a more efficient and user-friendly experience for consumers. The artificial intelligence system demonstrated the capacity to automatically resolve spelling errors, thereby exhibiting enhanced tolerance for errors when compared to conventional systems. A further favorable aspect is that the AI was able to accurately interpret synonyms, thereby identifying the correct products.

5.3 Limitations

The implementation of AI could be exploited by users with relative ease, provided they have some degree of experience with AI. In the user study, for instance, a user effectively replaced the system with the search bar and issued commands through it.

The search function implemented in the conventional system did not align with the prevailing technological standards. The search was exclusively based on textual descriptions, which is a limitation when attempting to emulate existing web shops. It is therefore recommended that a search function be implemented that aligns with contemporary technological standards to facilitate the emulation of modern web shops.

5.4 Future Work

In light of the limited diversity observed in user studies, it would be advisable to undertake a study that involves fewer participants, particularly those with a background in information technology. Additionally, it would be beneficial to include older adult groups to assess the intuitiveness of the artificial intelligence interface. This approach would facilitate a comprehensive evaluation of the ease of use of the AI for different demographics.

A further investigation could be conducted in which the conventional system and the AI are compared on two separate pages. This would allow for the assessment of the efficiency and efficacy of AI utilization in a web shop. This approach could also address the filter bias identified in our user study.

Due to temporal constraints, a static template was employed, with its sole reliance on the description. In this instance, the integration of a state-of-the-art template could potentially enhance the comparison.

Another aspect that must also be mentioned in this context is protecting the system from being exploited by users. It is essential to ensure that users cannot exercise any control over the AI.

5.5 Design Recommendations

6 Conclusions

References

[1] Henry Kautz Ana-Maria Popescu, Oren Etzioni. 2003. *Towards a Theory of Natural Language Interfaces to Databases.* https://dl.acm.org/doi/10.1145/604045.604070

[2] OWASP Foundation. 2024. *OWASP Top Ten | OWASP Foundation.* https://owasp.org/www-project-top-ten/

[3] Eve Rouse. 2023. *New research: 69straight to the search bar when visiting ecommerce sites, but 80to a poor experience.* https://www.nosto.com/blog/new-search-research/