Mid-Term Project Review 1 – Group 31 | Information Retrieval (CSE508) Winter 2024

App-Police: An Application Policy Summariser

Jahanvi Bakshi

IIIT Delhi

[jahanvi20069@iiitd.ac.in](mailto:jahanvi20069@iiitd.ac.in)

Prateek Mishra

IIIT Delhi

[prateek20102@iiitd.ac.in](mailto:prateek20102@iiitd.ac.in)

Yogesh Kaushik

IIIT Delhi

[yogesh20163@iiitd.ac.in](mailto:yogesh20163@iiitd.ac.in)

Ritik Kirar

IIIT Delhi

[ritik21413@iiitd.ac.in](mailto:ritik21413@iiitd.ac.in)

Shourya Singh

IIIT Delhi

[shourya21422@iiitd.ac.in](mailto:shourya21422@iiitd.ac.in)

Siddharth

IIIT Delhi

[siddharth21424@iiitd.ac.i](mailto:siddharth21424@iiitd.ac.in)n

# 1. Introduction

In the rapidly evolving digital landscape, mobile applications have become an integral part of our daily lives. However, these applications often come with lengthy and complex privacy policies that many users tend to overlook or find difficult to comprehend. This lack of understanding can lead to the misuse of personal data without the user's informed consent, raising significant concerns about digital privacy and security.

# 2. Problem Statement

The primary challenge addressed by App-Police is the need for a user-friendly solution that simplifies privacy policies and highlights the crucial points users need to know before agreeing to share their information. Many users skip over these policies due to their complexity and length, leaving them unaware of how their data will be used and potentially exposing them to privacy risks.

Gaining users' trust and developing an algorithm that can effectively distinguish between irrelevant and essential parts of a privacy policy are significant challenges in this project. Additionally, creating a system that can provide personalized recommendations for alternative applications based on user preferences and privacy scores adds another layer of complexity.

# 3. Literature Review

Numerous studies have focused on summarizing and identifying unsafe apps through the analysis of their privacy policies. Narseo Vallina-Rodriguez et al.'s paper [1] introduces PrivacyGrade, a methodology that evaluates smartphone apps' privacy behaviors by scrutinizing their privacy policies using automated technology. This approach demonstrates the potential for using machine learning techniques to assess the privacy risks associated with mobile applications.

Sushain Cherivirala et al.'s work [2] presents an approach utilizing natural language processing (NLP) techniques to extract insights from privacy policies and inform improved mobile app design. By identifying standard privacy practices concerning data collection, sharing, and retention, this study highlights the importance of clear and transparent communication of privacy policies to users.

Adwait Nadkarni et al. [3] scrutinize the privacy policies of popular Android VPN apps and pinpoint issues related to data collection, sharing, and retention. Their findings reveal that many apps lack clarity in disclosing their data practices, emphasizing the need for better privacy policy analysis and communication.

Narseo Vallina-Rodriguez et al. [4] expand upon the PrivacyGrade approach in their work "PrivacyScore," assessing the privacy behaviors of over 5,000 Android apps. Their results indicate that many apps inadequately disclose their data practices or provide misleading information, underscoring the importance of developing tools to help users make informed decisions about the apps they use.

While these studies showcase the potential of leveraging privacy policies to identify unsafe apps and improve privacy practices, challenges persist regarding the accuracy of automated tools and the transparency and understandability of privacy policies. App-Police aims to address these challenges by providing a user-centric solution that combines advanced information retrieval techniques with a focus on usability and transparency.

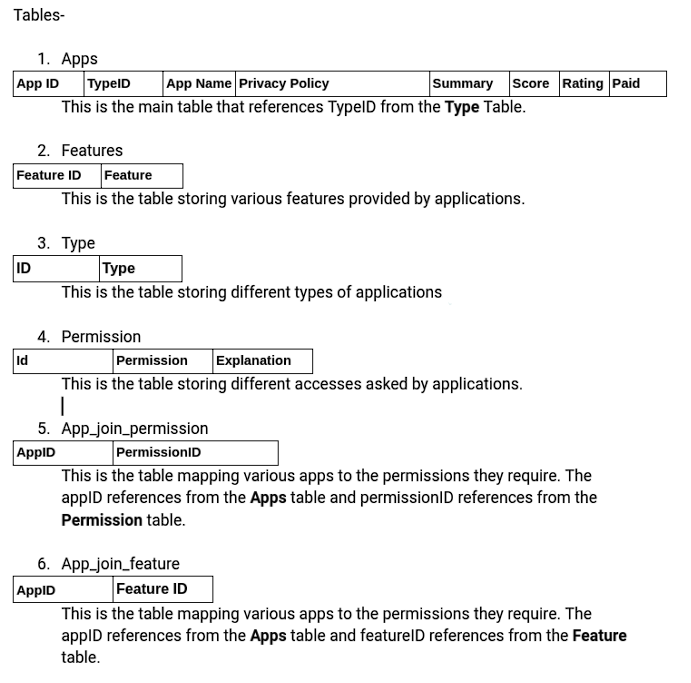
# 4. Methodology

## 4.1 Data Collection

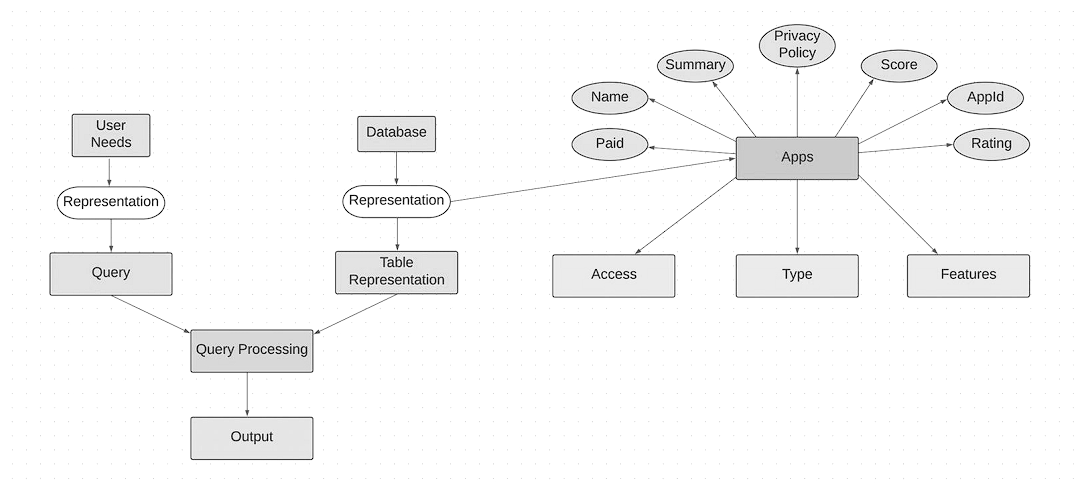
The data collection process for App-Police involves extracting privacy policy text from official documents associated with applications on the Google Play Store. This ensures that the analysis is based on the most up-to-date and accurate information provided by the app developers. Additionally, basic information regarding the permissions requested by the application upon installation is verified from the mobile device's settings and stored in our backend database for subsequent analysis.

## 4.2 Database Design

The backend database of App-Police is designed to store comprehensive information about the applications, including the permissions they request, their Play Store ratings, and the features they offer. This data serves as the foundation for the app's privacy policy analysis and personalized application recommendations. The database design is illustrated in the provided ER diagram, which showcases the relationships between the various entities and attributes.



*Figure 1.1: Schematic representation of database*



*Figure 1.2 ER diagram representation of database*

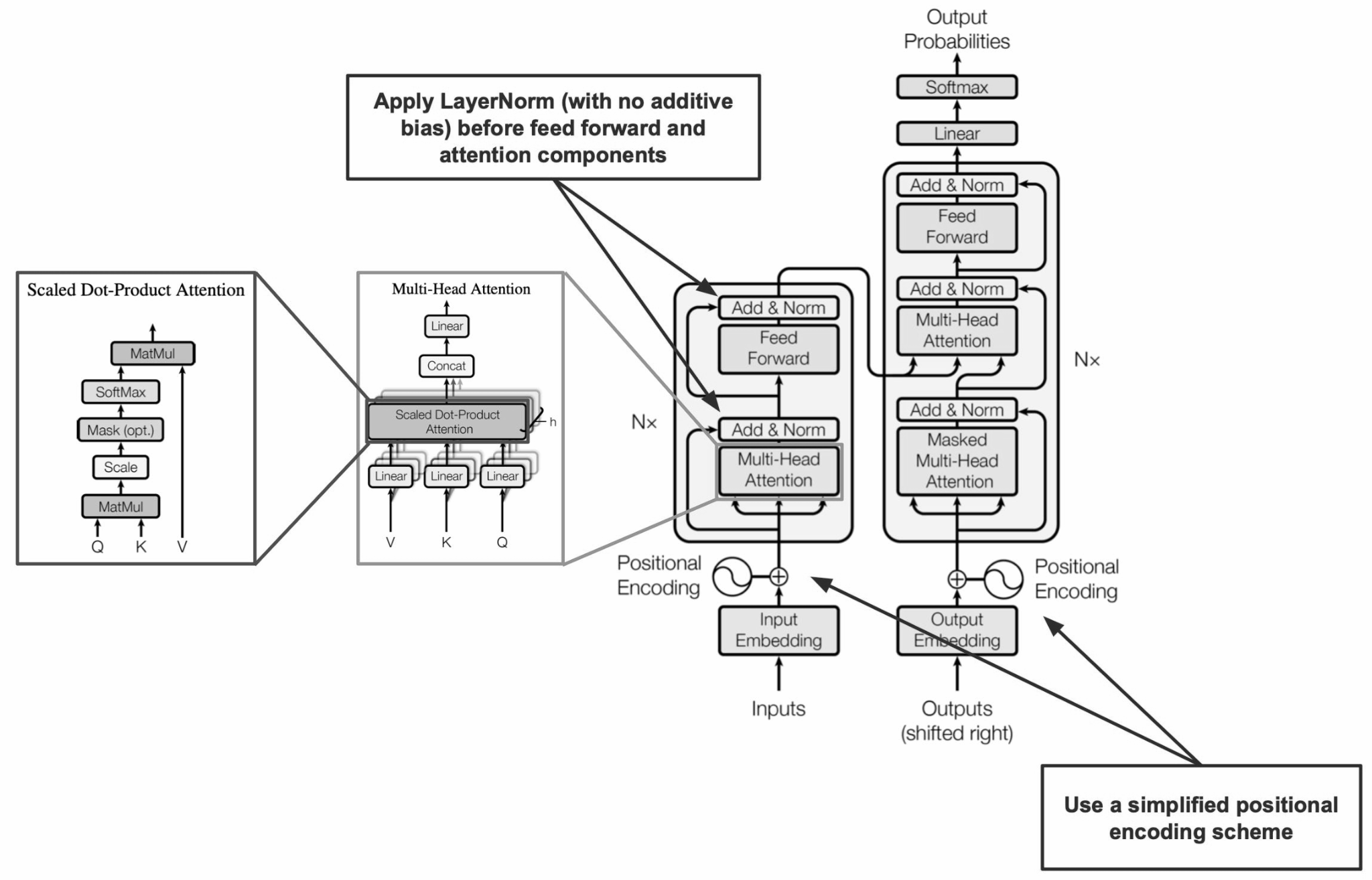
## 4.3 Information Retrieval Techniques

### 4.3.1 Text Preprocessing

To prepare the privacy policy text for summarization and analysis, App-Police employs several text preprocessing techniques. These include tokenization (breaking down the text into individual words or phrases), lemmatization (reducing words to their base or dictionary form), and the removal of punctuation marks and stop words (common words that do not contribute to the overall meaning). These preprocessing steps help to normalize the text and improve the accuracy of the subsequent analysis.

### 4.3.2 Text Summarization

App-Police utilizes the pre-trained "Transformer" model T5-BASE, developed by Google, for text summarization. T5 (Text-to-Text Transfer Transformer) is a state-of-the-art language model that has been trained on a vast corpus of text data and fine-tuned for various NLP tasks, including summarization. By leveraging this model, App-Police can generate concise and meaningful summaries of the privacy policies, highlighting the key points users need to be aware of.



*Figure 2: Schematic diagram of the T5 (text-to-text transfer transformer)*

### 4.3.3 Inverted Indexing

To enable efficient retrieval of relevant information, App-Police employs an inverted indexing technique. This involves creating an index that maps each word or phrase to the documents in which it appears. By using inverted indexing, the app can quickly locate and retrieve the specific parts of the privacy policies that mention keywords or phrases related to data collection, sharing, or other privacy concerns. This allows for faster and more accurate analysis of the privacy policies.

### 4.4 Collaborative Filtering

In addition to the summarization and analysis of privacy policies, App-Police incorporates a collaborative filtering system to provide personalized application recommendations to users. Collaborative filtering is a technique that makes predictions or recommendations based on the preferences and behaviors of similar users. By analyzing the privacy scores, app ratings, and user preferences, the system can suggest alternative applications that offer similar features while maintaining a higher level of data security. This helps users discover new apps that align with their needs and values without compromising their privacy.

### 4.5 Score Calculations

To assess the privacy and safety of an app, App-Police utilizes a weighted sum approach in its baseline evaluation. The app is categorized into three groups: "secure," "unsafe," and "moderate," based on the presence and frequency of specific keywords related to user privacy. These keywords include terms such as "data collection," "third-party sharing," "advertising," and others that indicate potential privacy risks. The overall app score is determined by calculating the weighted sum of the occurrences of these keywords in the privacy policy summary. This score provides users with a quick and easy-to-understand assessment of the app's privacy practices.

# 5. Baseline Results (Updated)

## 5.1 System Design

The information regarding various permissions requested by the application, the play store rating of the app, and its features are stored in our database, which will be utilized for the final application recommendation. Prior to this, we pre-processed the data by employing various techniques such as tokenisation, lemmatisation, and removal of punctuation marks, among others. For text summarisation, we utilized the pre-trained "Transformer" model T5-BASE to summarize the privacy policies of different applications. The T5 (Text-to-Text Transfer Transformer) model is a transformer-based language model developed by Google and trained on a large amount of diverse text data. It was fine-tuned on various natural language processing (NLP) tasks, such as question-answering, summarisation, and language generation. The architecture of the T5 model is based on the transformer model, which is a neural network capable of processing sequential data like text.

The T5 architecture comprises an encoder-decoder structure, wherein the encoder converts the input sequence into a fixed-length vector representation. On the other hand, the decoder utilizes the encoder output along with a task-specific prompt to generate the final output sequence. To determine whether the current application is safe for our baseline evaluation, we employ weighted sums. This is achieved by classifying the application into three categories, namely "secure", "unsafe", and "moderate". We then extract the summary of the privacy policy for the app and generate a list of keywords related to user privacy, such as "data collection", "third-party sharing", "advertising", among others. Subsequently, we calculate the number of occurrences of each keyword and assign weights to each keyword based on its significance in user privacy. Finally, we calculate the overall app score based on the weighted sum of the keyword occurrences.

The baseline model has been changed in various ways. The summarizer was working well so that has been kept the same way. We have changed the way in which the privacy score was being calculated. Unlike before, when we categorized apps into 3 categories namely secure, unsafe and moderate, we now are giving a privacy score for which the value ranges from 0 to 10. The calculation for the privacy score is done using a function. In this function, we take the number of apps 'n' as an input and a list of dictionaries. In this list, the first dictionary has the app names as key values and the occurrence of the first 'special word' as its value. These special words are words with high information about the threat level of an app. The intermediate weights for a specific special word and a specific app are calculated by dividing that word's occurrence in the app's privacy policy by the total number of occurrences of all the special words. After that, for each special word, these intermediate weights are multiplied by the occurrences of them in all different apps and then summed up. With this, we get weights for each specific word returned in the 'score\_list. Moreover, we have equipped our model with a functional user interface to enable interaction with our model. It has been explained in detail in the subsequent parts.

## 5.2 Evaluation

We also analyzed the working of our application by manually analyzing the summarizes produced by our model and seeing if they provide a quick and complete review of the privacy policy of the application by comparing it to manually summarized versions.

Along with the privacy score, we used another evaluation metric to gather user feedback using a surveying mechanism. A google form was floated amongst our friends, family, and peers. This form gathered basic information about their behavior relating to privacy policies and data breaches. Further, we tried to gauge whether users would be willing to use an app with the functionality that Pol - I - See promises to offer. These were some of the insights from the survey -

How often do you read the privacy policy of the apps you download?

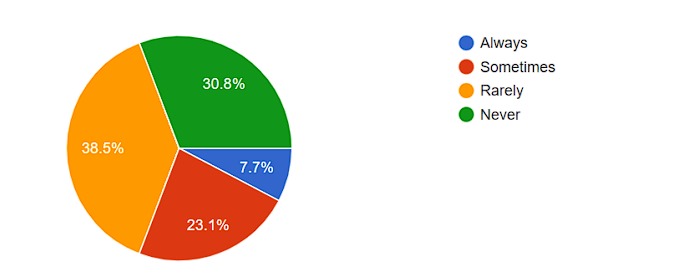


Figure 2.1: Highlighting user tendency towards privacy policy

Would you be interested in an app/website that summarizes the privacy policies of different apps on the Play Store?

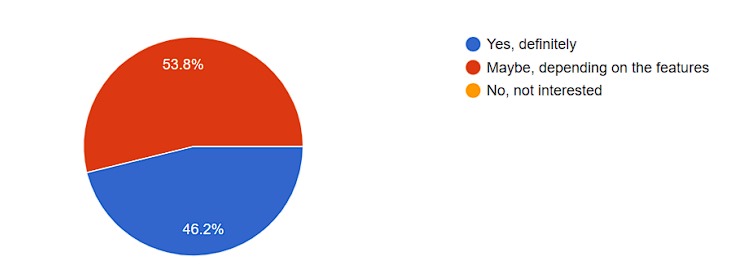


Figure 2.2: Highlighting user attitude towards App Police

How important is the safety score of an app to you?

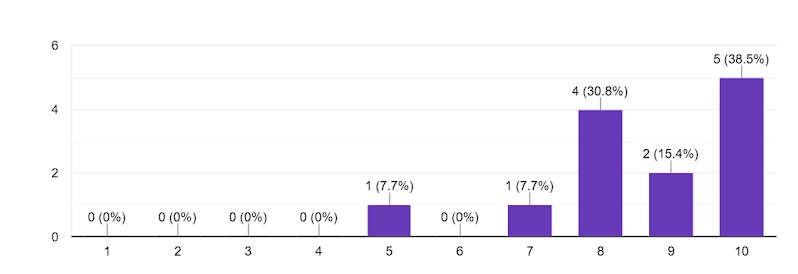
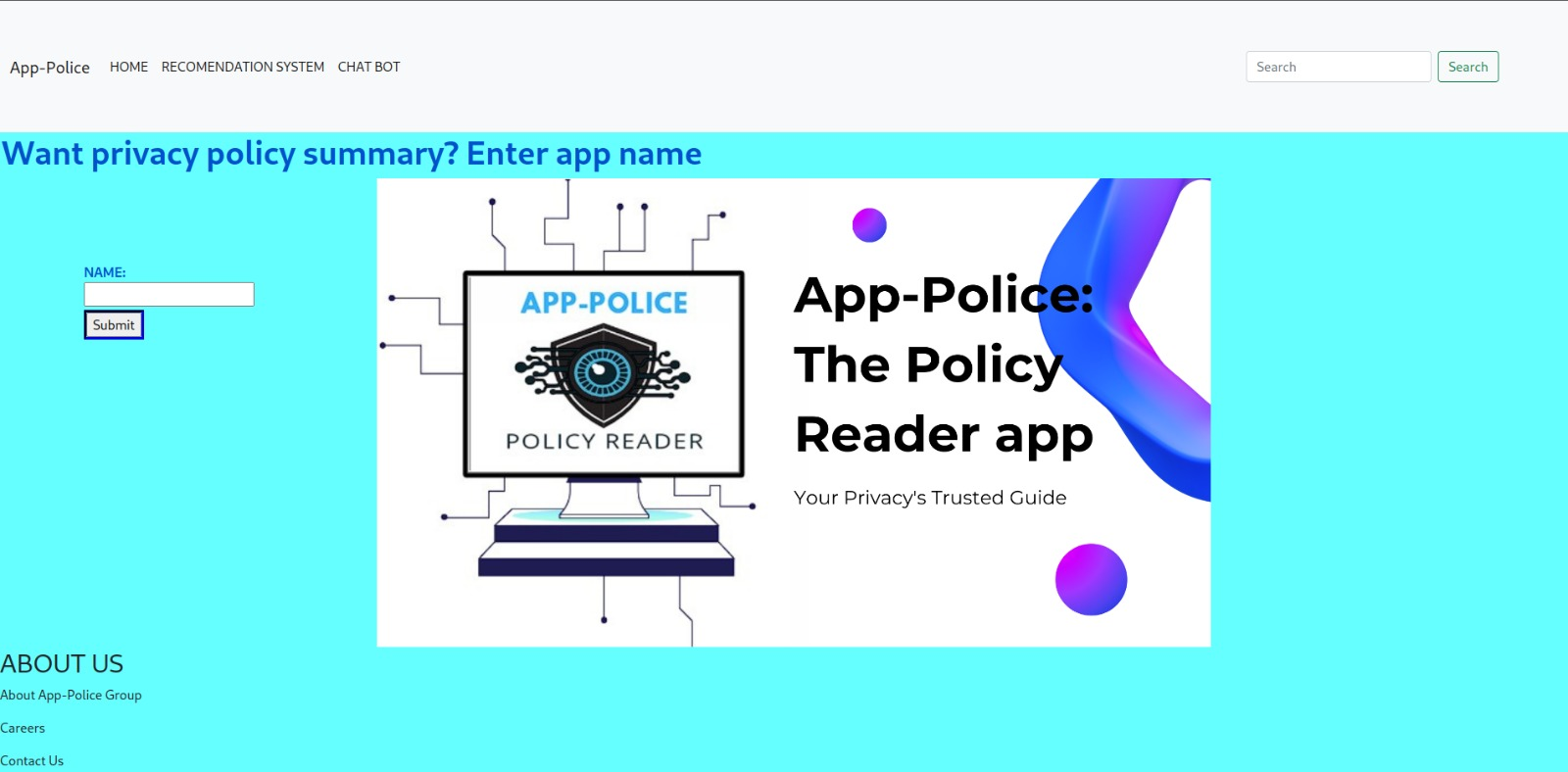
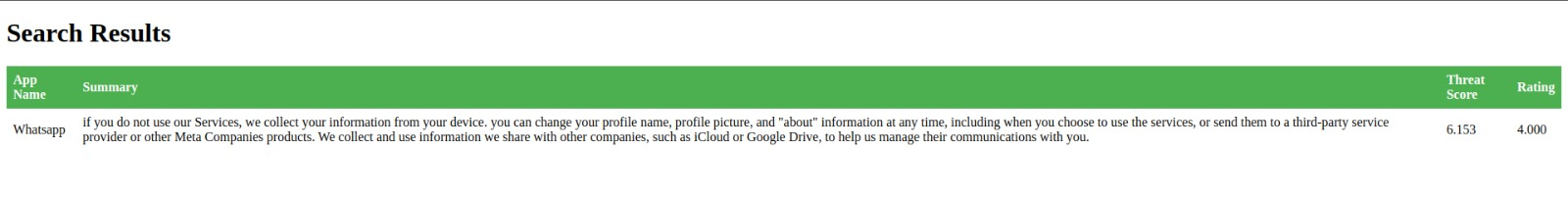


Figure 2.3: Highlighting the importance of app safety score for the users

## 5.3 Frontend

Below are the snippets from the currently working frontend:





# 6. Future Scope

While the current prototype of App-Police demonstrates significant potential in addressing the challenges of privacy policy comprehension and safe app discovery, there is ample room for further development and improvement. Future work will focus on several key areas:

## 6.1 Algorithm Refinement

Continuously refining the algorithms used for text summarization, collaborative filtering, and score calculations is crucial to improving the accuracy and effectiveness of the app. This involves incorporating user feedback, analyzing larger datasets, and exploring advanced machine learning techniques to enhance the app's performance.

## 6.2 Database Expansion

Expanding the database to include a wider range of applications across different platforms (e.g., iOS, web-based apps) will provide users with a more comprehensive overview of the privacy landscape. Collaborating with app developers and privacy experts to ensure the accuracy and completeness of the database is essential for maintaining the app's reliability.

## 6.3 User Feedback Integration

Incorporating user feedback is vital for understanding the real-world effectiveness of App-Police and identifying areas for improvement. Implementing mechanisms for users to provide ratings, comments, and suggestions within the app will help to refine the user experience and ensure that the app continues to meet the evolving needs and expectations of its users.

## 6.4 Multi-language Support

To make App-Police accessible to a global audience, future versions of the app should include support for multiple languages. This involves translating the app interface, privacy policy summaries, and chatbot responses to cater to users from different linguistic backgrounds.

## 6.5 Integration with App Stores

Collaborating with app store providers to integrate App-Police's privacy scores and recommendations directly into the app store interfaces could significantly enhance the app's reach and impact. This would allow users to access privacy insights and alternative app suggestions seamlessly while browsing and installing apps.

# 7. Conclusion

App-Police represents a significant step forward in empowering users to make informed decisions about their digital privacy. By leveraging advanced information retrieval techniques, collaborative filtering, and user-centric design, the app aims to create a safer and more transparent digital experience for everyone. The baseline results demonstrate the effectiveness of the proposed methodology, while the future scope highlights the potential for continued improvement and expansion.

# 8. References

[1] Vallina-Rodriguez, N., et al. (2015). Privacygrade: Measuring the privacy behaviors of smartphone apps. In Privacy Enhancing Technologies Symposium.

[2] Cherivirala, S., et al. (2017). Mining privacy policies for better mobile app design. IEEE Transactions on Software Engineering, 43(9), 834–848.

[3] Nadkarni, A., et al. (2018). Privacy policy analysis of android VPN apps. In IEEE European Symposium on Security and Privacy Workshops.

[4] Vallina-Rodriguez, N., et al. (2017). Privacyscore: Analyzing the privacy behaviors of smartphone apps at scale. In IEEE Symposium on Security and Privacy.