App Police

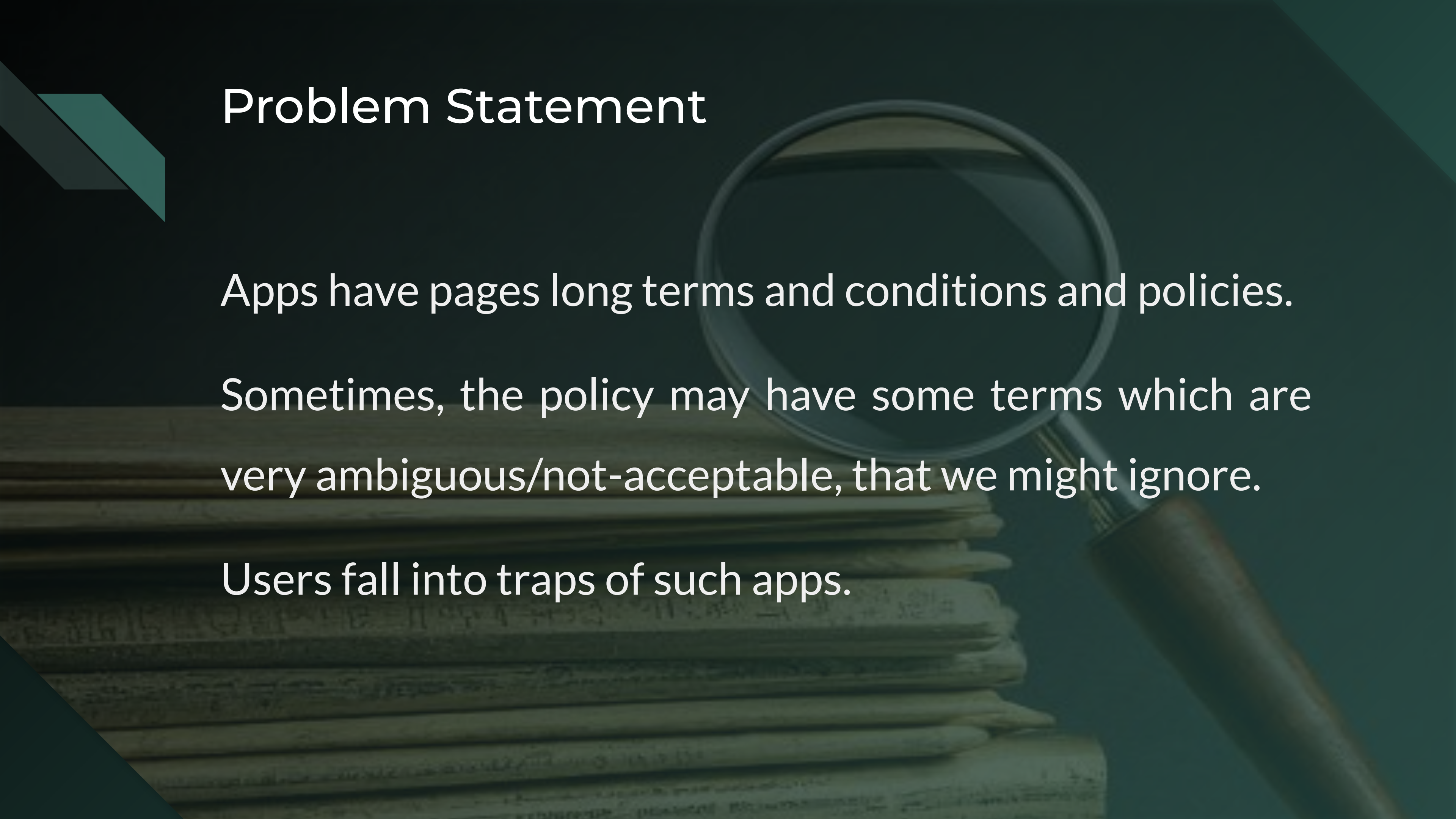
The Policy Reader App

GROUP 31

Jahanvi Bakshi (2020069), Prateek Mishra (2020102)
Yogesh Kaushik (2020163), Ritik Kirar (2021413)
Shourya Singh (2021422), Siddharth (2021424)

INTRODUCTION

Problem Statement



Apps have pages long terms and conditions and policies.

Sometimes, the policy may have some terms which are very ambiguous/not-acceptable, that we might ignore.

Users fall into traps of such apps.

Motivation and Challenges

- Privacy policies outlines how a company collects, uses, and shares our personal information
- By skipping it, we may not know how your data is being used and who it is being shared with.
- This can leave us vulnerable to identity theft, data breaches, and other privacy violations
- Second, a privacy policy may contain important information about our rights and personal data.

Existing Apps

LexCheck

Seal

Evisort

LIMITATIONS

User have to provide the URL of the privacy policy for the service.

Focus on data collection; neglect areas like data usage and sharing practices.

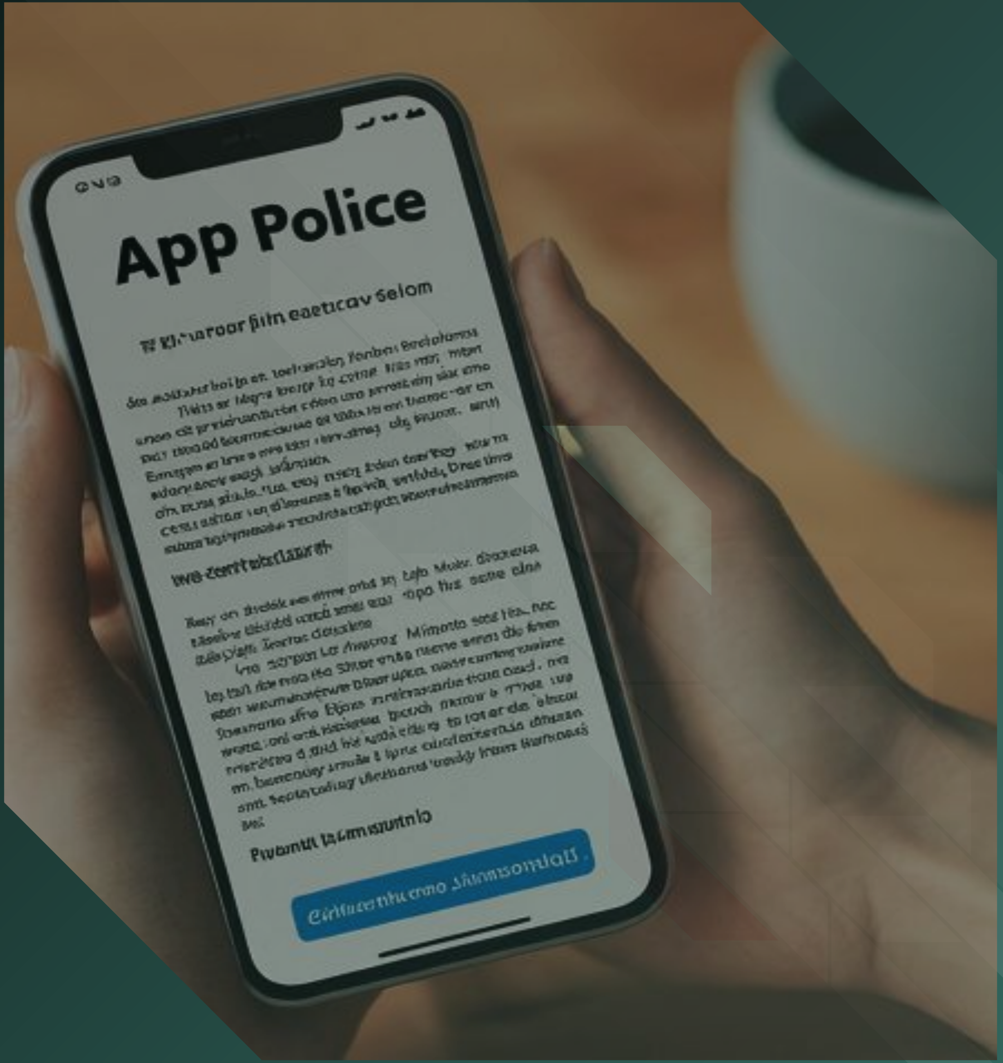
Literature Review

PrivacyGrade: Evaluates apps' privacy behaviors through policy analysis. [1]

Mining Privacy Policies: Utilizes NLP to identify standard privacy practices for app design improvement. [2]

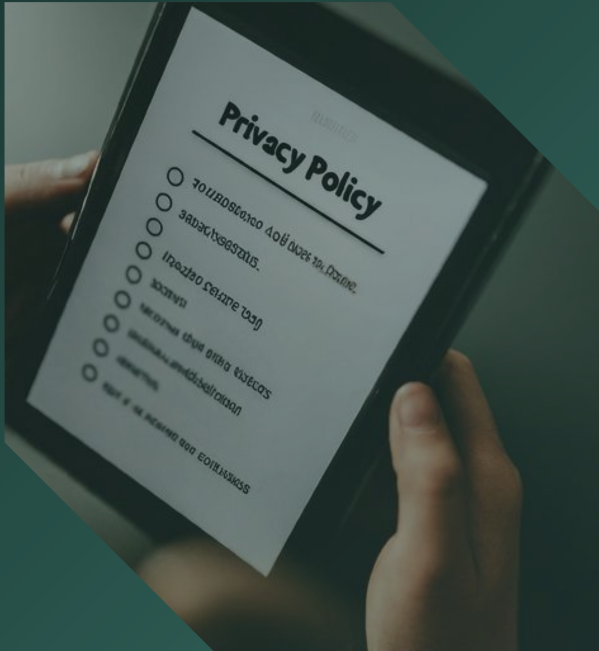
Privacy Policy Analysis : Pinpoints data privacy issues in VPN app policies. [3] [4]

App Police



Proposed Solution

- Automatic Privacy Policy Summarization and Safety Classification
- Recommendations for Safer Apps
- Chatbot Support for Seamless Interaction



Features

Text Summarization: Utilizes LLMs for concise policy summaries.

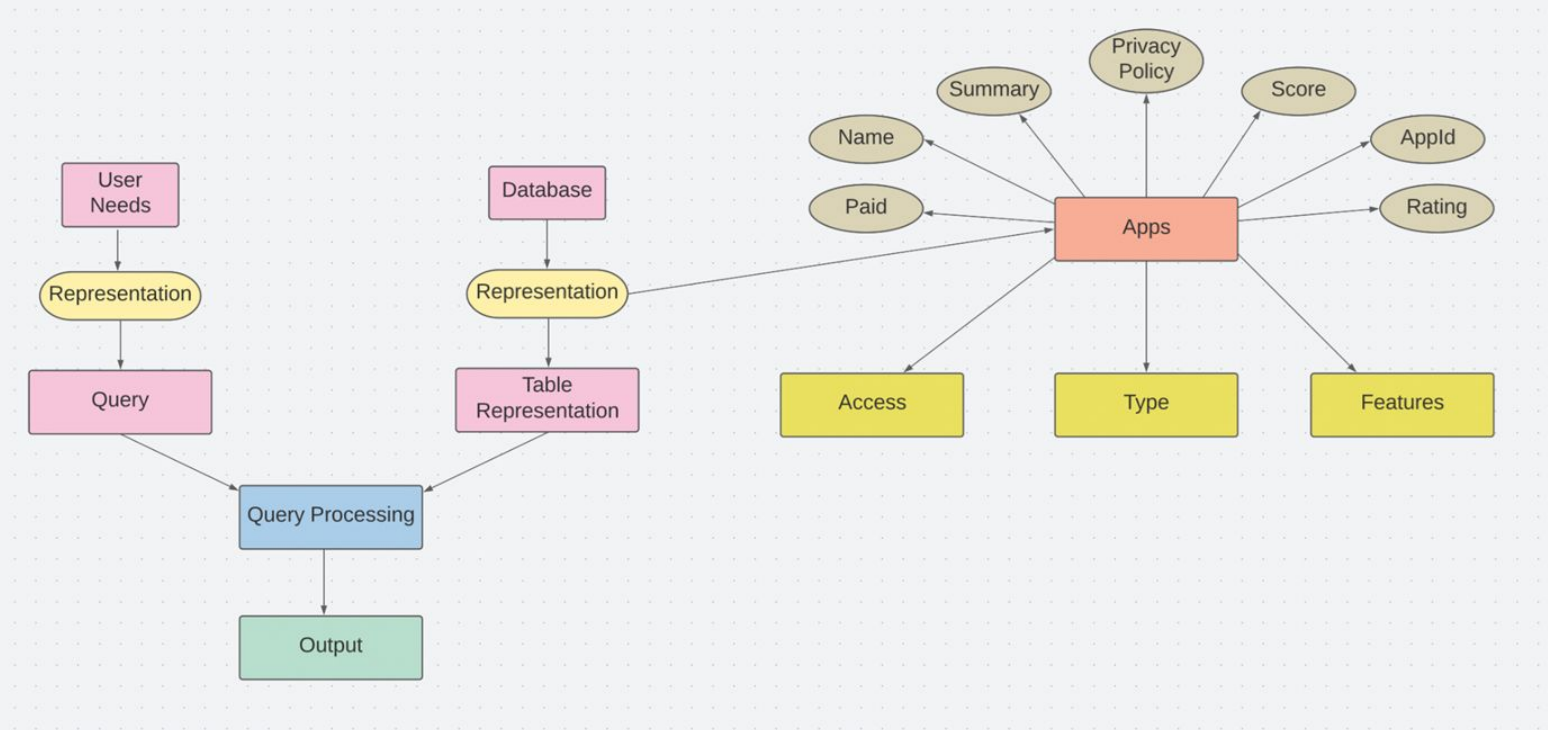
Privacy Score Calculations: Categorizes apps into secure, unsafe, and moderate based on privacy policy analysis.

App Recommendation: Recommends more safer, similar apps to the users.

Chat Bot: Chatbot delivers precise and prompt responses to user inquiries.

Upto Baseline Results

WorkFlow


Privacy Policy
Summary
Score
Name
AppId
User Needs
Database
Paid
Apps
Rating
Representation
Representation
Query
Table Representation
Access
Type
Features
Query Processing
Output

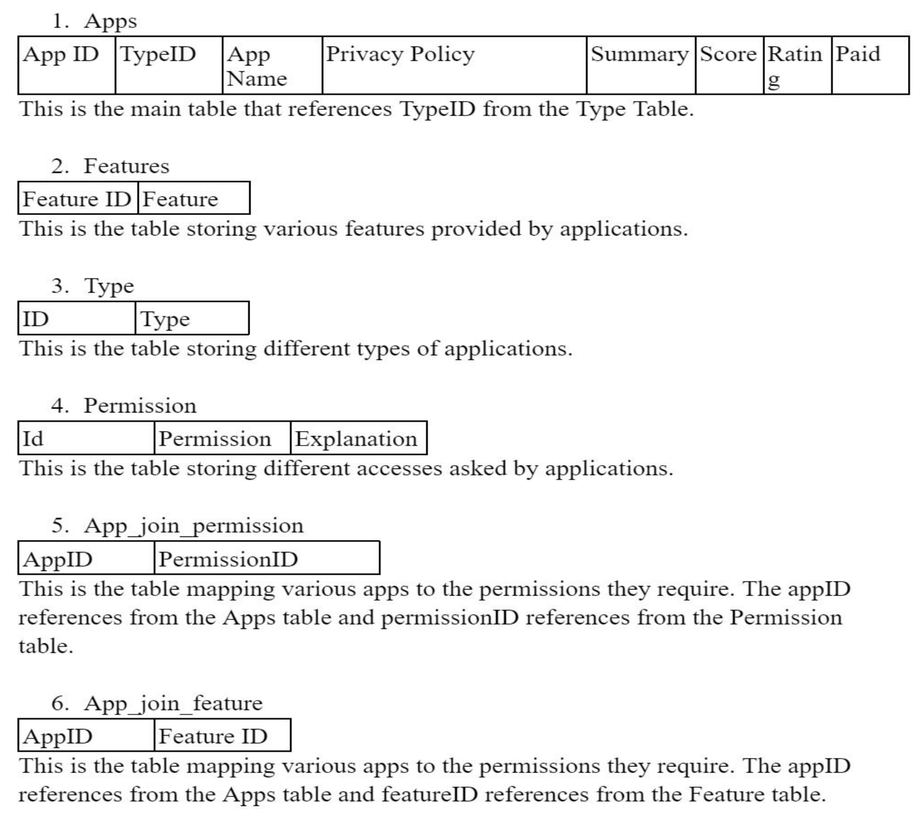
Data Collection

For the App-Police application, the text for the Privacy Policy has been taken from the official Privacy Policy document linked to the application from Google Play Store. These privacy policy documents are available on the internet as well for various applications.

We have stored some data in our database and for better retrieval positional and inverted index have been created for permissions, features and other categories of information and for privacy policy text.

Database

App-Police's backend database holds key app details like permissions, ratings, and features, crucial for policy analysis and recommendations. Illustrated via an ER diagram, it ensures efficient functionality.



1. Apps

App ID	TypeID	App Name	Privacy Policy	Summary	Score	Rating	Paid

This is the main table that references TypeID from the Type Table.

2. Features

Feature ID	Feature

This is the table storing various features provided by applications.

3. Type

ID	Type

This is the table storing different types of applications.

4. Permission

Id	Permission	Explanation

This is the table storing different accesses asked by applications.

5. App_join_permission

AppID	PermissionID

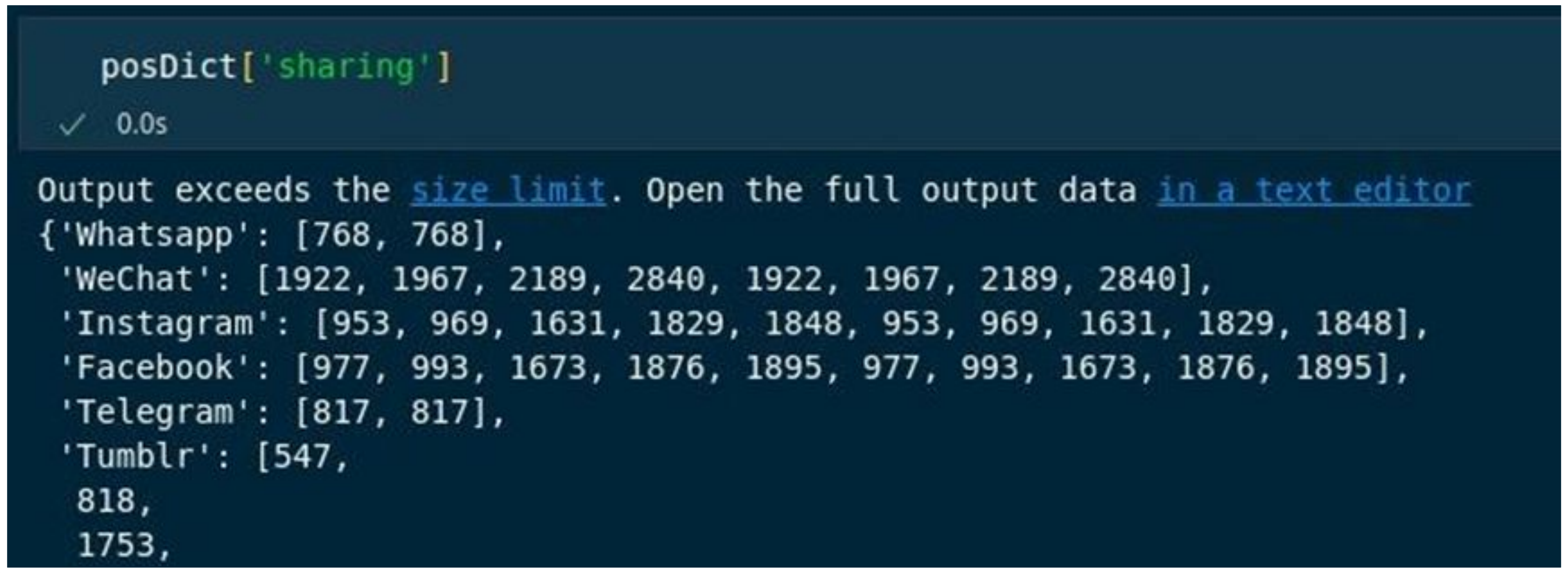
This is the table mapping various apps to the permissions they require. The appID references from the Apps table and permissionID references from the Permission table.

6. App_join_feature

AppID	Feature ID

This is the table mapping various apps to the permissions they require. The appID references from the Apps table and featureID references from the Feature table.

Inverted Positional index to store features and permissions



```
posDict['sharing']
```

```
Output exceeds the size limit. Open the full output data in a text editor
{'Whatsapp': [768, 768],
 'WeChat': [1922, 1967, 2189, 2840, 1922, 1967, 2189, 2840],
 'Instagram': [953, 969, 1631, 1829, 1848, 953, 969, 1631, 1829, 1848],
 'Facebook': [977, 993, 1673, 1876, 1895, 977, 993, 1673, 1876, 1895],
 'Telegram': [817, 817],
 'Tumblr': [547,
  818,
  1753,
```

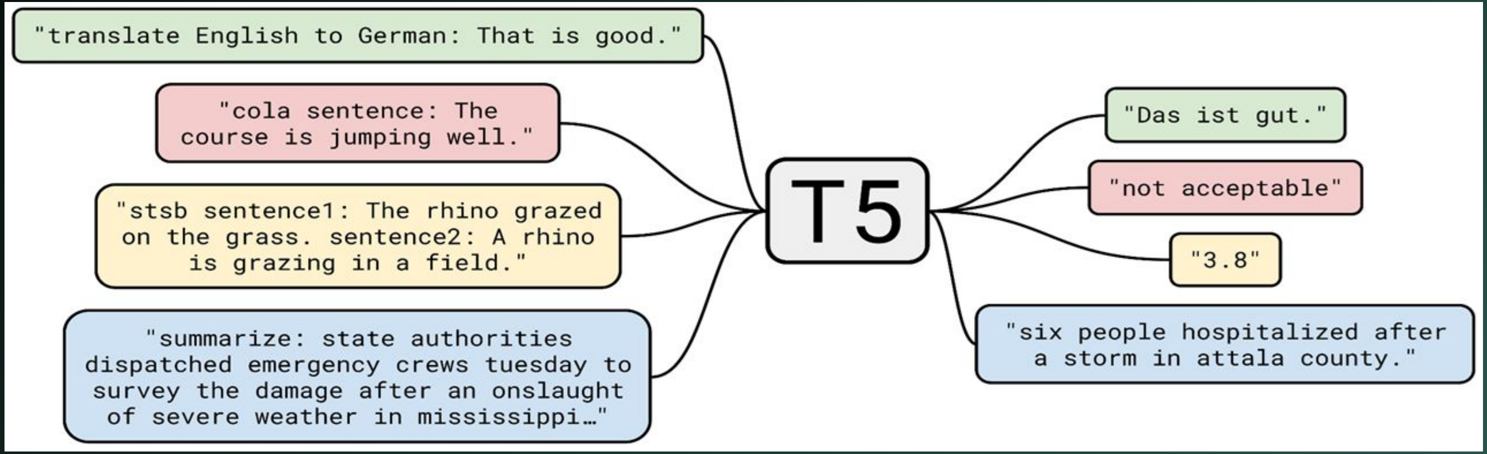
Summarization

Keywords were extracted from app privacy policies using **Countvectorizer** for unigram features, then word embeddings were obtained using the 'all-mpnet-base-v2' sentence transformer.

Cosine similarity was applied to match specific keywords to each app's document, enhancing relevance.

T5-Small, a pre-trained transformer-based language model, was utilized to summarize app privacy policies. Keywords were added as prefixes to increase their importance in the summary, resulting in a more balanced output.

T5 Transformer - Baseline Model



"translate English to German: That is good."

"cola sentence: The course is jumping well."

"stsb sentence1: The rhino grazed on the grass. sentence2: A rhino is grazing in a field."

"summarize: state authorities dispatched emergency crews tuesday to survey the damage after an onslaught of severe weather in mississippi…"

"Das ist gut."

"not acceptable"

"3.8"

"six people hospitalized after a storm in attala county."

App-Police employs Google's T5-BASE Transformer model for text summarization, generating concise privacy policy summaries that highlight key points for user awareness.

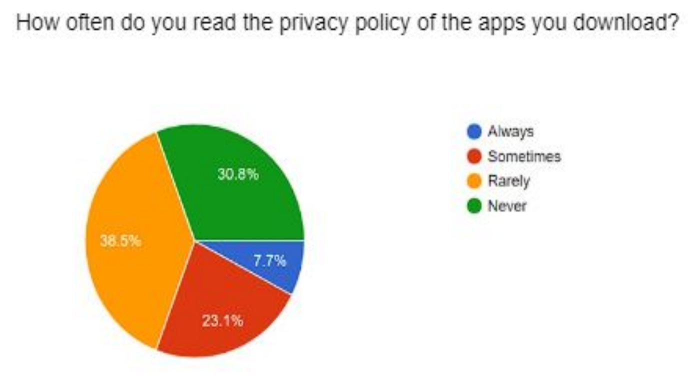
Threat Score

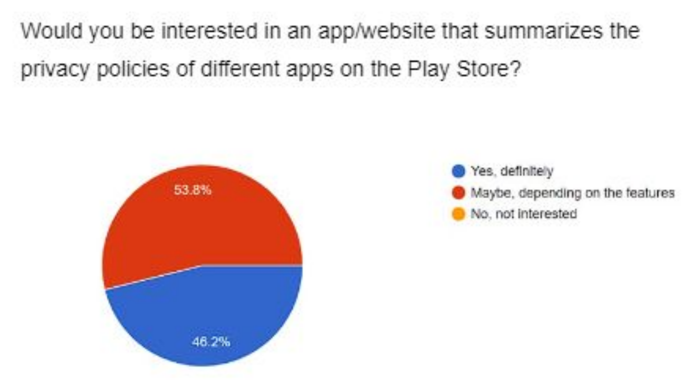
For threat score calculation evaluation, apps are categorized as "secure", "unsafe", or "moderate" using weighted sums, we now are giving privacy score for which the value ranges from 0 to 10. Privacy policy summaries are analyzed for keywords like "data collection" and "advertising", assigning weights based on significance for user privacy. App scores are calculated accordingly.

User Studies

User studies highlight the attitudes of users towards privacy and safety. A majority of users showed negative attitudes towards reading long user policies, but showed interest in an application that would summarize the policies for them.

[Google form Link]


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


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

Novelty

Our system provides summarized versions of app privacy policies and assigns **safety scores** from 0 to 10.

It offers **recommendations for safer apps** based on a database, promoting user transparency and understanding.

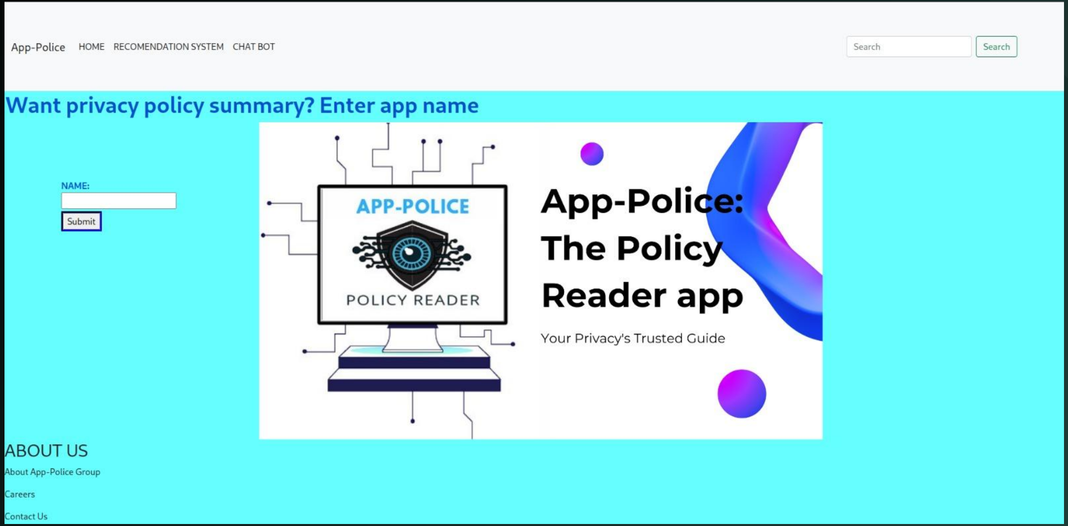
Our application includes a **chatbot for user interaction** and support, facilitating easy access to information and assistance.

Expected Impact

- Increased comprehension of app privacy policy
- Promote **transparency** and ethical operations
- Effective compliance with laws and regulations related to privacy policies.
- Improve user trust in applications
- Save time and effort for both users and companies

Final Submission

Front-End Interface



Want privacy policy summary? Enter app name

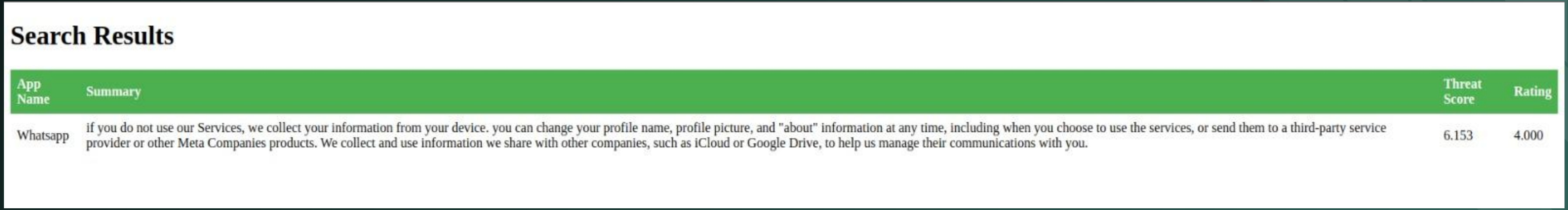
ABOUT US

About App-Police Group

Careers

Contact Us

Summarization Results



Search Results

App Name	Summary	Threat Score	Rating
Whatsapp	if you do not use our Services, we collect your information from your device. you can change your profile name, profile picture, and "about" information at any time, including when you choose to use the services, or send them to a third-party service provider or other Meta Companies products. We collect and use information we share with other companies, such as iCloud or Google Drive, to help us manage their communications with you.	6.153	4.000

EVALUATION

For our evaluation we simply use weighted sums to determine whether the current app is safe or not.

Define a list of keywords that relate to user privacy, such as "data collection", "third-party sharing", "advertising" etc.

Extract the summary of the privacy policy for the app.

Calculate the number of occurrences of each keyword in the summary.

Assign a weight to each keyword based on its importance in terms of user privacy.

Calculate the overall app score based on the weighted sum of the keyword occurrences.

Performance evaluation for summarizer

We have used to metrics for our evaluation:

ROUGE (Recall-Oriented Understudy for Gisting Evaluation): ROUGE is a set of metrics that measures the overlap between the generated summary and the reference summary in terms of n-gram matches. It computes precision, recall, and F1 scores.

OBTAINED ROUGE SCORE OF :- 0.65

BLEU (Bilingual Evaluation Understudy): BLEU measures the similarity between the generated summary and the reference summary in terms of n-gram matches. It computes precision, recall, and a geometric mean of these two scores.

OBTAINED BLEU SCORE :- 0.7

Performance evaluation for summarizer

For the summarization task we have calculated Rouge and Bleu scores for different pretrained models like gpt-2,gemini and T5.

We also tried to use lamma but due to computational constraints we can't get the scores .

MODEL	Rouge	Bleu-
GPT 2	0.48	0.45
Gemini	0.54	0.51
T5	0.65	0.7

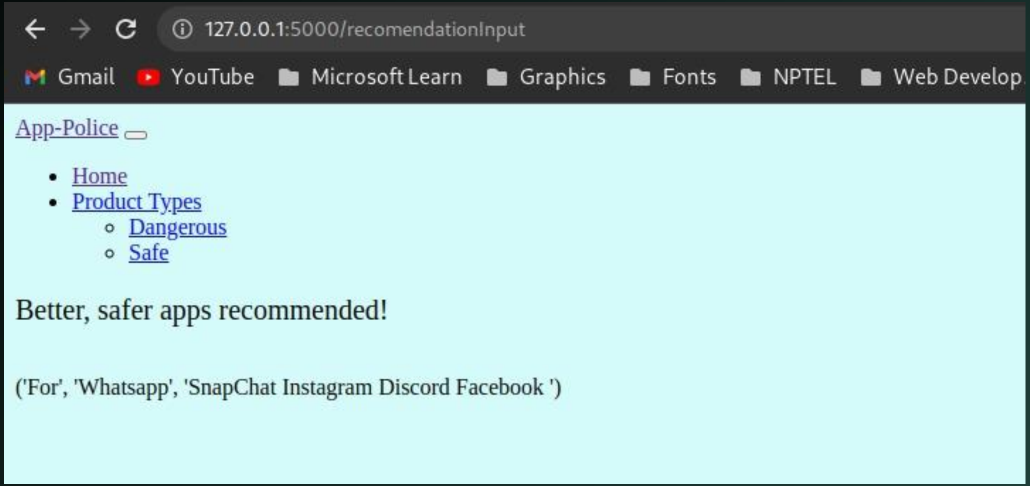
RECOMMENDER SYSTEM

Our application integrates a built-in recommendation system designed to suggest safer alternatives upon the installation of a new app. This recommendation system utilizes the Jaccard similarity metric to quantify the similarity between the feature vectors of the newly installed app and those already present in our database. The feature vector comprises all distinct feature IDs found within the app.

We compute a score for each app stored in the database, categorizing them as either safe or unsafe. Utilizing this score and considering the degree of similarity between the newly installed app and the apps within our database, our system provides recommendations for apps that are not only similar but also deemed safer.

The score assigned to each app is inversely related to its safety level; hence, a lower score indicates a safer app. Consequently, our system offers alternative recommendations to users that are deemed safer than the currently installed app.

Recommender



App-Police

- Home
- Product Types
  - Dangerous
  - Safe

Better, safer apps recommended!

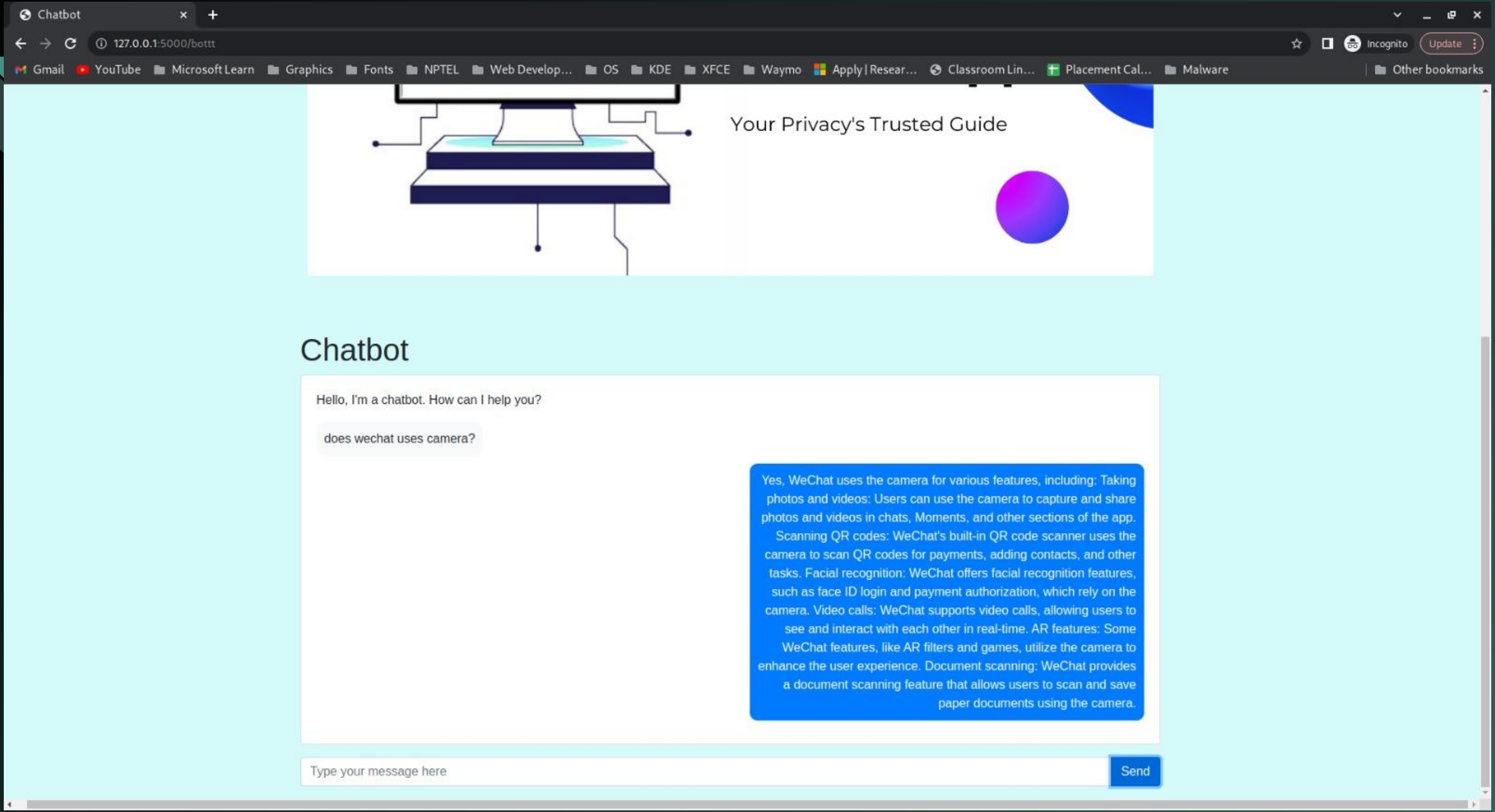
('For', 'Whatsapp', 'SnapChat Instagram Discord Facebook ')

Here, as we can see when asked for recommendations for Whatsapp we get SnapChat, Instagram, Discord and Facebook which according to our score evaluator are safer apps.

CHATBOT

Our application features a chatbot powered by the Gemini API, which has been fine-tuned using data from our privacy policy. This enables the chatbot to deliver precise and prompt responses to user inquiries, while also demonstrating our dedication to safeguarding their personal data.

By training the Gemini model on this preprocessed data, our chatbot has gained a comprehensive understanding of our privacy policy guidelines.



Chatbot

Hello, I'm a chatbot. How can I help you?

does wechat uses camera?

Yes, WeChat uses the camera for various features, including: Taking photos and videos: Users can use the camera to capture and share photos and videos in chats, Moments, and other sections of the app. Scanning QR codes: WeChat's built-in QR code scanner uses the camera to scan QR codes for payments, adding contacts, and other tasks. Facial recognition: WeChat offers facial recognition features, such as face ID login and payment authorization, which rely on the camera. Video calls: WeChat supports video calls, allowing users to see and interact with each other in real-time. AR features: Some WeChat features, like AR filters and games, utilize the camera to enhance the user experience. Document scanning: WeChat provides a document scanning feature that allows users to scan and save paper documents using the camera.

Contributions

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.

THANK YOU