Mid Project Review

INFORMATION RETRIEVAL

CSE 508

Samriddh Singh	Aaditya Gupta	Harjeet Singh Yadav
2020466	2020552	2020561

Ishita Sindhwani	Diya Ahuja	Varun Parashar
2020305	2020431	2020482

PROBLEM FORMULATION -

The aim of our project is to develop an app/website that simplifies the process of reading privacy policies by providing a summarized version of crucial aspects that users need to know before granting access to their personal information. We aim to address the growing concern about digital privacy and protect users from potential data exploitation. Our algorithm will utilize keywords to identify critical points in the policy, and we will optimize it to ensure a safer digital experience for users. Additionally, we will generate a safety score for each application based on the data collected in our database and incorporate play store ratings and application reviews to suggest alternate apps with similar features. Going forward, we also aim to increase our data corpus and utilize web scraping in order for the app to be able to access privacy policies from the Internet and summarize along with providing a privacy score. Our primary goal is to establish trust with users by being transparent and seeking legitimacy through app testing agencies.

LITERATURE REVIEW -

Privacy policies are documents of a complex nature that elucidate the methodology adopted by an application or website for collecting, using, and distributing user data. The policies, which are typically lengthy and riddled with legal jargon, demand considerable effort from users to comprehend the data being collected and how it is utilized. In recent years, growing concerns regarding user privacy and data protection have led to increased research on simplifying privacy policies and enhancing their comprehensibility for the average user.

Several studies have been conducted to analyze the readability of privacy policies. In a 2011 study by Aleecia M. McDonald and Lorrie Faith Cranor, the authors found that the average privacy policy on a website required a college undergraduate level of reading ability, thereby making it difficult for the average user to understand. In another study in 2017 by Hana Habib and Yunan Chen, the privacy policies of the top 20 apps on the Google Play Store were analyzed, and it was found that most of these policies were written at a level beyond the recommended 8th-grade level.

Several tools have been developed to assist users in understanding privacy policies. The Usable Privacy Policy Project (UPP), for instance, is a tool developed by Lorrie Faith Cranor and her team at Carnegie Mellon University that analyzes privacy policies and provides a summary of the key points in plain language. The

Privacy Assistant is a browser extension that provides users with a summary of the privacy policy of the website they are visiting.
Several companies have developed their own systems for rating the safety and privacy of apps. For example, Google Play Protect is a service provided by Google that scans apps for malware and other security issues before they are downloaded onto a user's device. Similarly, AV-TEST is an independent organization that tests and rates antivirus and security software.
Several app discovery platforms allow users to search for apps based on specific features or functionality. The Google Play Store and Apple's App Store, for instance, have a "related apps" section that suggests apps similar to the one a user is currently viewing. Third-party app discovery platforms such as AppBrain and AppCrawlr also enable users to search for apps based on specific features or functionality.
In conclusion, significant research and development efforts have been made around privacy policies and app safety ratings. While several tools have been developed to assist users in understanding privacy policies and evaluating the safety of apps, there is still a need for a comprehensive solution that combines these features and provides users with an easy-to-understand summary of the privacy policies of different apps on the Play Store.

UPDATED BASELINE RESULTS -System and Prototype

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.

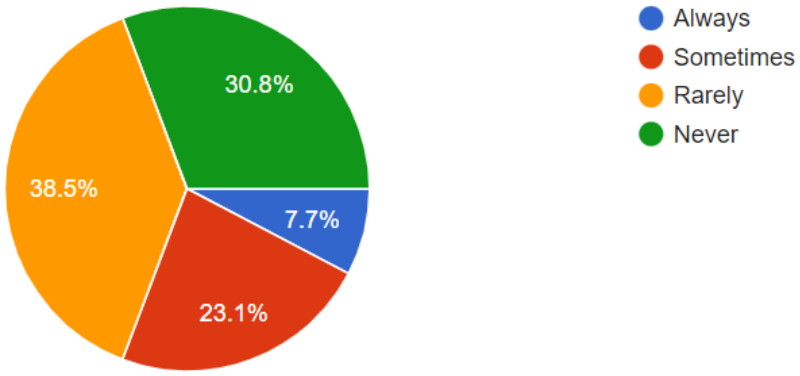
The baseline model has been changed in various ways. The summarizer was working well so that has been kept the same way. We have changed the way in which the privacy score was being calculated. Unlike before, when we categorized apps into 3 categories namely secure, unsafe and moderate, we now are giving 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.

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

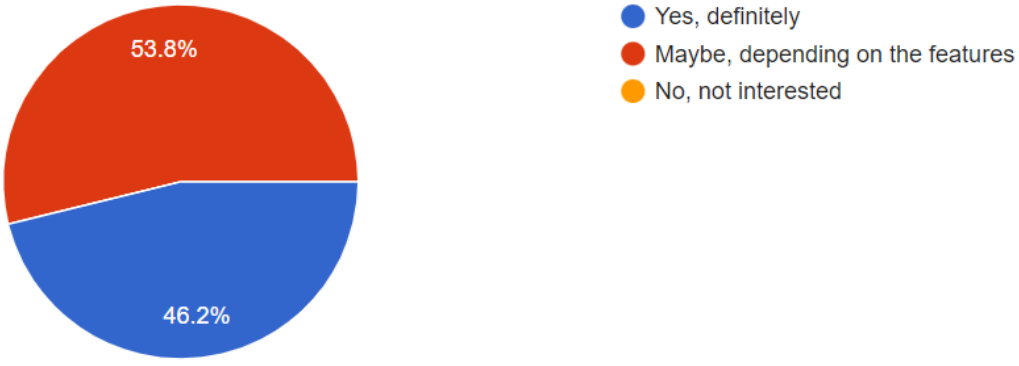
complete review of the privacy policy of the application by comparing it to manually summarized versions.

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 -

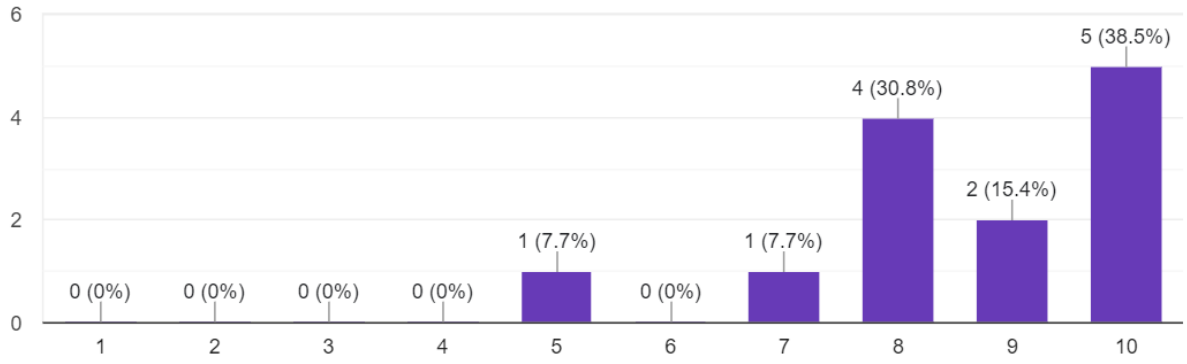
Q: How often do you read the privacy policies of the apps you download?



Q: Would you be interested in an app/website that summarizes the privacy policies of different apps on the Play Store and provides a safety score for each app?



Q: How important (on a scale of 1-10) is the safety score of an app to you when downloading it?



Link to the form - https://forms.gle/R1EN8SLNGuVhFPow5

PROPOSED METHODS - Data Analysis, Features and future works

Our project aims to develop a web application that simplifies the process of reading privacy policies, which often prove lengthy and complex, causing users to skip them. Our solution involves providing users with a summarized version of the policies, highlighting the crucial aspects that they need to know before granting access to their personal information. Our primary motivation for this project is to safeguard users from digital predators who exploit their data without consent. We are aware of the challenges in building trust with users and developing an algorithm capable of distinguishing between irrelevant and essential parts of a privacy policy. To address these challenges, we plan to be transparent with our users and seek legitimacy through app testing agencies. Our algorithm will utilize keywords to identify critical points in the policy, and we will optimize it at every stage to ensure a safer digital experience for users in the future. We intend to generate a score based on the data collected in our database to determine the safety of an application. Moreover, depending on the user's requirements for desired features, our application will suggest applications that meet those needs while maintaining a good privacy score. Additionally, it will incorporate play store ratings and application reviews into the recommendations.

In our current model, our software application prompts users to specify the name of the application they wish to assess. Upon input, the application generates a succinct summary of the privacy policy, emphasizing crucial points that users ought to be mindful of. Furthermore, it provides a privacy score that indicates the extent to which the application intrudes upon user data, determined by analyzing the

frequency of particular keywords. Additionally, we intend to introduce a feature that displays the average privacy score for an application category within our dataset.
Our website will also offer the functionality that recommends applications with favorable privacy scores to users who input specific features they are seeking in an application. This allows users to identify applications that serve their purposes without compromising their personal data. We plan to include an artificial intelligence-based chatbot that will be trained on privacy policy data to answer user queries. Moreover, we intend to incorporate web scraping, enabling us to search the internet and update our database with additional applications, thereby expanding the range of options and meeting user needs.

In addition, we intend to leverage other pertinent information about the application to enhance the recommendations provided to the user. Currently, the recommendation system relies solely on the privacy score derived from the analysis of the application's privacy policy. However, incorporating details such as the application's Play Store rating and pricing status can provide users with a more comprehensive view of the application's overall review, allowing them to make more informed decisions. These features will be incorporated into our system by our final deadline.
We have also planned to utilize the Jaccard coefficient for the implementation of a recommendation system based on features and app permissions. The applications with a higher Jaccard coefficient will be more likely to be recommended.

Our data was collected from the official privacy policy documents of the Google Play Store. Further, our database provides basic information about these applications, like their features, permissions, price, etc.
The data is stored in our backend and can be found here for interpretation and analysis:
https://docs.google.com/spreadsheets/d/1rzbxkkpa5jS6y2a4eGOP09lvH_8SgEOyI-ZD2YH1ZQc/edit?usp=sharing
The layout of the database sufficed our needs, thus it has not been tampered with.

Database Tables -

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.

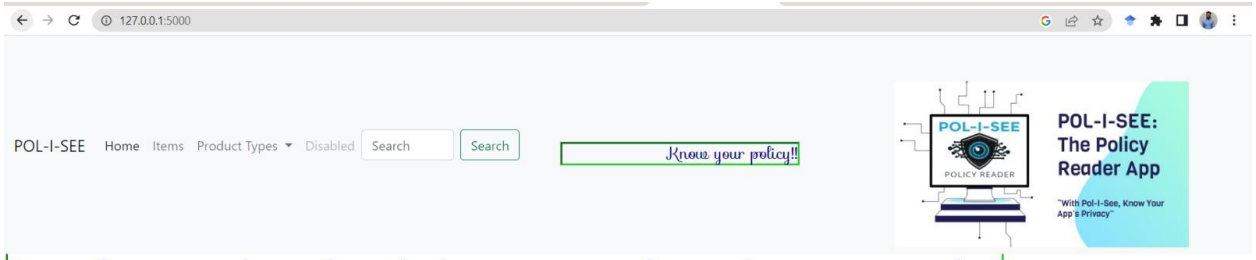
6. App_join_feature

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.

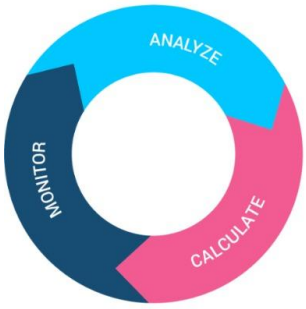
At present, we have developed a rudimentary backend and frontend to facilitate user interaction with our system. However, we plan to improve these components in subsequent development stages.

These screenshots show the current state of our website:



Enter the name of app for which you want to know their privacy policy

Name: Submit



App With their privacy score

App With their privacy score

Safe Apps and Dangerous App

App With their Ratings

Ratings

Reveal!!

ABOUT US

About POL-I-SEE Group

Careers

Contact Us

POL-I-SEE People

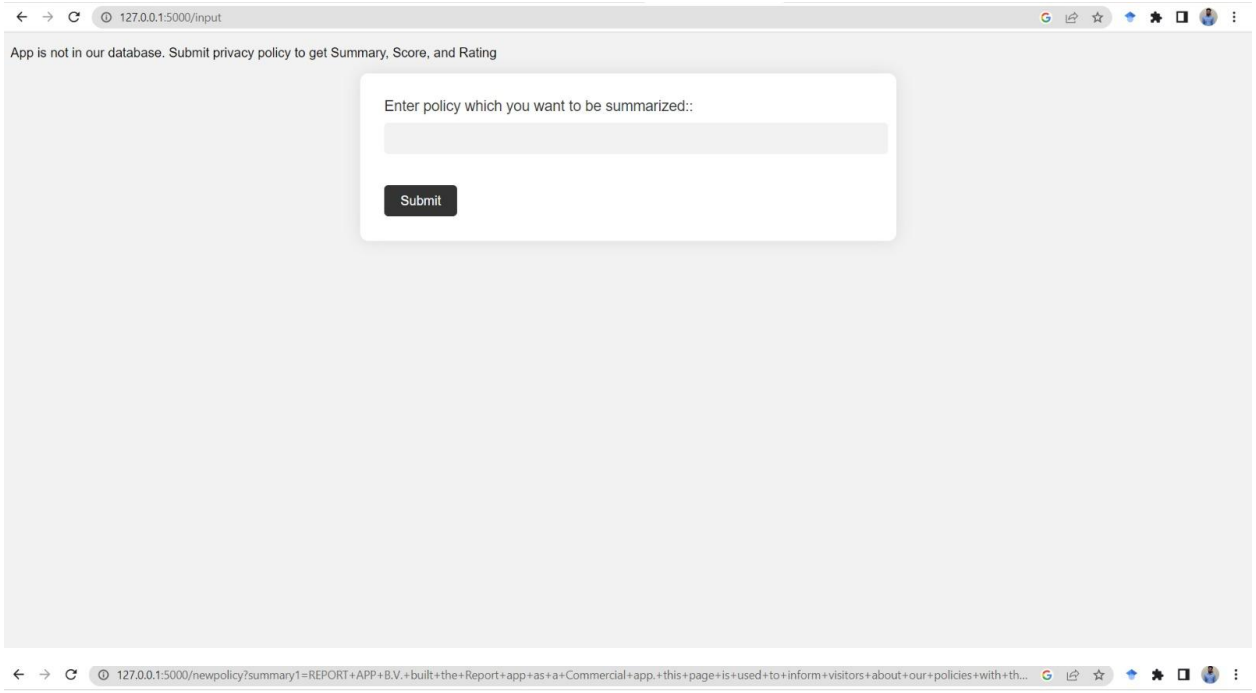
Help

Legal & Privacy information

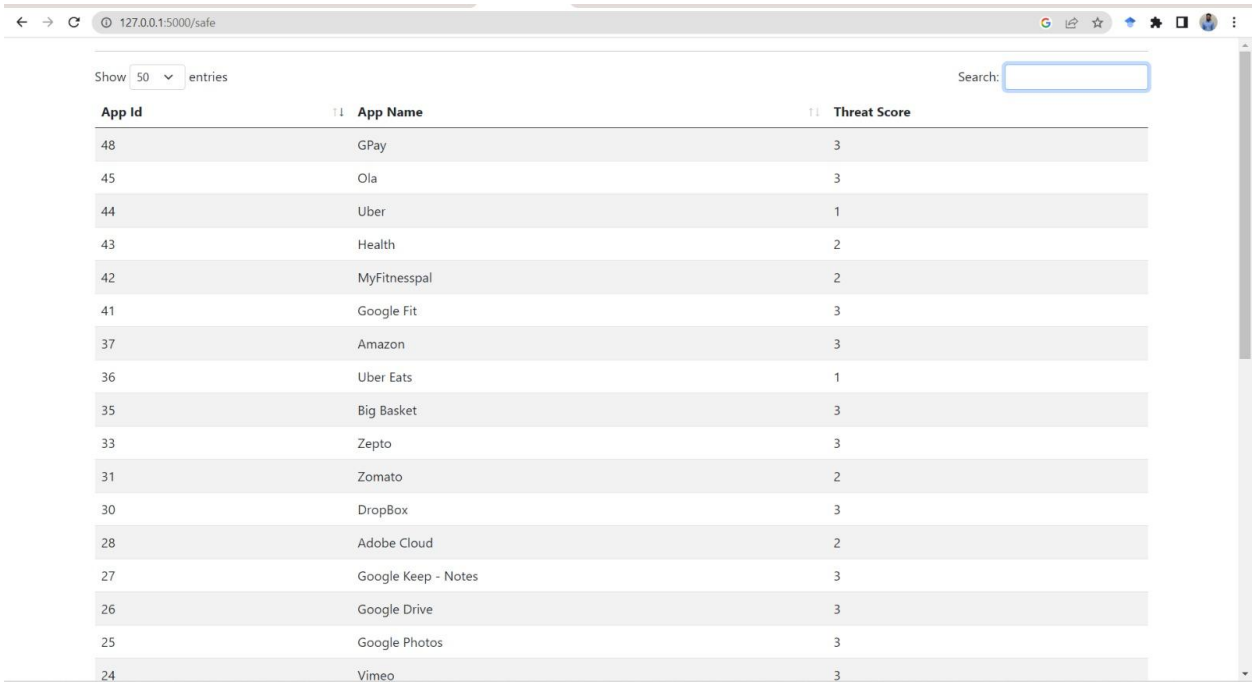
Blog

Search Results

App Name	Summary	Threat Score	Rating
Whatsapp	we collect and share your information to help us operate, provide, improve, understand, customize, support, and market our Services. if you choose to use our services, we may collect information about you, including your phone number, profile picture, or "about" information, which is stored on our servers for up to 30 days, as we try to deliver them.	3	4



Summary	Privacy Score
REPORT APP B.V. built the Report app as a Commercial app. this page is used to inform visitors about our policies with the collection, use, and disclosure of Personal Information if anyone chose to use our Service - but we will not use or share your information with anyone except as described in this Privacy Policy 'cookies'It's Privacy Score is:: 10.090167453842852	10.090167453842852


127.0.0.1:5000/safe
Show 50 entries
Search:
App Id
App Name
Threat Score
48 GPay 3
45 Ola 3
44 Uber 1
43 Health 2
42 MyFitnesspal 2
41 Google Fit 3
37 Amazon 3
36 Uber Eats 1
35 Big Basket 3
33 Zepto 3
31 Zomato 2
30 DropBox 3
28 Adobe Cloud 2
27 Google Keep - Notes 3
26 Google Drive 3
25 Google Photos 3
24 Vimeo 3