POL-I-SEE(Baseline Results)

Samriddh Singh
IIIT
samriddh20466@iiitd.ac.in
Delhi, India

Varun Parashar
IIIT
varun20482@iiitd.ac.in
Delhi, India

Aaditya Gupta
IIIT
aaditya20552@iiitd.ac.in
Delhi, India

Harjeet Singh Yadav
IIIT
harjeet20561@iiitd.ac.in
Delhi, India

Diya Ahuja
IIIT
diya20431@iiitd.ac.in
Delhi, India

Ishita Sindhwani
IIIT
ishita20305@iiitd.ac.in
Delhi, India

March 13, 2023

1 Problem Statement

Our project aims to develop an app that simplifies the process of reading privacy policies, which many people tend to skip due to their length and complexity. Our web app will provide a summarized version of the policies, highlighting the crucial aspects that users need to know before granting the app access to their personal information. Our primary motivation behind this project is to protect users from digital predators who exploit their data without their consent. We acknowledge the challenge of building trust with users and creating an algorithm distinguishing between irrelevant and essential parts of a privacy policy. To address these challenges, we propose 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. We will optimize it at every stage to ensure a safer digital experience for users in the future. A score to decide how safe an application is will be generated based on the data collected in our database. Moreover, depending on the requirements of the user in terms of what features they want, our application will suggest applications that meet those needs while maintaining a good privacy score. In addition to this, it will also incorporate the play store ratings and application reviews for the recommendations.

2 Literature Review

There exist numerous works on summarizing and identifying unsafe apps using their privacy policies. For instance, "PrivacyGrade: Measuring the Privacy Behaviors of Smartphone Apps" by Narseo Vallina-Rodriguez, et al.[1] proposes a methodology that assesses the privacy behaviors of smartphone apps by analyzing their privacy policies. The authors developed PrivacyGrade, which uses automated technology to read privacy policies and rate apps based on their privacy practices. In another work, "Mining Privacy Policies for Better Mobile App Design" by Sushain Cherivirala, et al.[2] the authors present an approach that uses natural language processing techniques to extract information from privacy policies. They identify standard privacy practices related to data collection, sharing, and retention, which helps design better mobile apps. Additionally, "Privacy Policy Analysis of Android VPN Apps" by Adwait Nadkarni et al.[3] analyzes the privacy policies of popular Android VPN apps and identifies data collection, sharing, and retention issues. The authors found that many VPN apps failed to provide clear information on their data practices, with some even collecting sensitive information without users' knowledge or consent. Moreover, "PrivacyScore: Analyzing the Privacy Behaviors of Smartphone Apps at Scale" by Narseo Vallina-Rodriguez, et al.[4] extends the PrivacyGrade methodology to analyse the privacy behaviors of a large number of smartphone apps. The authors used PrivacyScore to examine the privacy policies of over 5,000 Android apps and discovered that many apps did not adequately disclose their data practices or offered misleading information. In addition to this, there are app recommender systems like AppCrawlr, which

recommend applications across platforms based on features required by the users. This can be extended to build a recommender system integrated with the summariser, which recommends apps with similar features and relatively safer privacy policies, if feasible. While these works demonstrate the potential of using privacy policies to identify unsafe apps and enhance privacy practices, there still need to be challenges regarding the accuracy of automated tools and the transparency and comprehensibility of privacy policies.

3 Baseline Results

3.1 Data Collections

Data has been collected from various sources. For the pol-i-see 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. Moreover, for our database general information about what permissions the application asks for when we install it is checked from settings of the mobile device.This data is stored in our backend database and is used for further analysis.

3.2 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

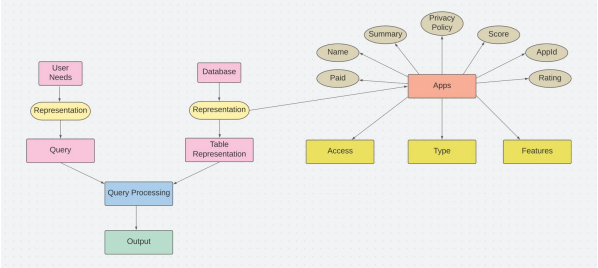
AppID	PermissionID

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.



ER diagram of our database

3.3 Summarizations

The information about various permissions asked by the application, the play store rating of the app, and the features it provides are stored in our database. This will be used for the final application recommendation. First, we have pre-processed the data with steps like tokenization, lemmatization, removal of punctuation marks etc. For text summarisation, we have used the Pre-trained "Transformer" model T5-BASE to summarize the privacy policies of different Apps. The T5 (Text-to-Text Transfer Transformer) model is a pre-trained transformer-based language model developed by Google. The T5-BASE model was trained on a massive amount of diverse text data and was fine-tuned on a wide range of natural language processing (NLP) tasks, such as question-answering, summarisation, and language generation. Its architecture is based on the transformer model, a type of neural network that can process sequential data like text. The T5 architecture is based on the transformer model and consists of an encoder-decoder structure. The encoder converts the input sequence into a fixed-length vector representation. At the same time, the decoder uses the encoder output along with a task-specific prompt to generate the final output sequence.

3.4 Score calculations

We simply use weighted sums to determine whether the current app is safe for our baseline evaluation. We do this by classifying the application into three categories: "secure", "unsafe", and moderate. Then, a list of keywords that relate to user privacy, such as "data collection", "third-party sharing", "advertising", etc. The summary of the privacy policy for the app is then extracted. In summary, the number of occurrences of each keyword is calculated, and weights are assigned to each keyword based on its importance in user privacy. Calculate the overall app score based on the weighted sum of the keyword occurrences.

References

[1] N. Vallina-Rodriguez, R. Balebako, M. Moreno, Y. Grinberg, H. Almuhimedi, N. Sundaresan, A. Felt, I. Aad, and N. Sadeh, "Privacygrade: Measuring the privacy behaviors of smartphone apps," *Privacy Enhancing Technologies Symposium*, 2015.

[2] S. Cherivirala, Y. Zhang, A. Iyengar, and L. Cranor, "Mining privacy policies for better mobile app design," *IEEE Transactions on Software Engineering*, vol. 43, no. 9, pp. 834–848, 2017.

[3] A. Nadkarni, P. Yadav, and A. Prakash, "Privacy policy analysis of android vpn apps," *IEEE European Symposium on Security and Privacy Workshops*, 2018.

[4] N. Vallina-Rodriguez, B. Reaves, A. Shah, N. Sundaresan, C. Kreibich, A. Felt, and V. Paxson, "Privacyscore: Analyzing the privacy behaviors of smartphone apps at scale," *IEEE Symposium on Security and Privacy*, 2017.