Sharing Machine Learning Models To Provide Personalized Experience Across Apps

Amir Hussain Memon

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
https://www.tdcommons.org/dpubs_series/3641

This work is licensed under a Creative Commons Attribution 4.0 License. This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Sharing Machine Learning Models To Provide Personalized Experience Across Apps

ABSTRACT

Users utilize multiple software applications on their devices. Currently, with user permission, each app can utilize user activity data to personalize the user’s experience of using the app. This disclosure describes techniques to securely provide a machine learning model (or other types of predictive model) trained on user activity in a particular app to one or more other apps on the same device. The model can then be used on the same device by the other apps to generate personalized rankings or recommendations for the user, without having access to user activity data. Personalization in this manner can improve the user experience of using apps. The described techniques are implemented with specific user permission and in compliance with applicable regulations.

KEYWORDS

- Personalization
- Recommendation
- Personalized ranking
- Encrypted model
- Machine Learning
- Mobile app
- User preference

BACKGROUND

Many software providers distribute multiple applications, e.g., mobile apps, that can be installed on a user device. For example, a single provider may distribute a browser app, a content sharing app, a payments app, etc. Each app typically has specific usage terms, including user privacy settings. With user permission, each app may have access to a user’s activity data within the app and may utilize the user’s activity for various purposes, e.g., providing recommendations, storing history (e.g., watch history, search history, browsing history, etc.). If the user permits, the
app may utilize such data to draw insights into the user’s needs, interests, or preferences. For example, the app may train a machine learning model based on the activity data. The usage of user activity data and the ML model is usually restricted to the specific app and such data is not available to other apps, even from the same software provider.

DESCRIPTION

This disclosure describes techniques to securely provide a machine learning model (or other types of predictive model) trained on user activity in a particular app to one or more other apps on the same device. The techniques are implemented with specific user permission and the user is provided options to disable such model sharing. Fig. 1 illustrates an example of implementation.

![Fig. 1: Process for making relevant recommendations by using data across applications](image-url)
As shown in Fig. 1, a user device (120) includes two apps (App 1, App2). The user device is in communication with a server 130. For example, the server 130 may be provided by the provider of App 1 or App 2, or may be an independent server. It is presumed that the user has provided permission to train an ML model based on activity data within App 1 and that the user permits other apps to utilize the trained ML model, after securely receiving the model.

For the purpose of illustration, consider that App 1 is a browser and App 2 a video viewing application, both executing on the user device. The user utilizes App 1 for routine browsing activity, e.g., to browse news websites, click on and read some articles, etc. With the user’s permission, the browsing activity within App 1 is utilized to train (102) a ML model locally, on-device. The model can be utilized to receive input data (e.g., user activity data) and generate predictions, e.g., recommendations of items for the specific user.

After training, the trained model is encrypted (104) and the encrypted payload is sent (106) to the server. For example, App 1 can encrypt the model using a private key, such that the model cannot be utilized without decryption, e.g., using a corresponding public key. The public key is shared (108) with App 2. For example, such sharing is performed such that the key never leaves the user device, e.g., via an on-device key-storage mechanism that is provided by a device operating system, by sharing a URL with the target app, etc.) or if the user permits, via a secure server (different from the server that receives the encrypted payload).

With user permission, the encrypted model is downloaded (110) by App 2 and is decrypted (112) using the public key obtained from App 1. The video viewing application App 2 can provide data to the trained ML model (e.g., a list of videos available to the user) and can receive corresponding output (e.g., a personalized ranking of the videos for the user). Based on the results, App 2 can then provide a user interface, e.g., the personalized ranked list of videos.
Other personalized experiences, e.g., smart suggestions, product recommendations, etc. can also be provided using the ML model.

In this manner, if the user permits, ML models (or other types of prediction techniques) that are trained on user activity in a particular application can be shared with another application, such that the user may receive a personalized experience without sharing actual user data with the other application. At no point in the process does user data leave the user device. Further, since the ML model is encrypted and secure key sharing mechanisms are used, the ML model is only usable on the user device.

While the foregoing discussion refers to a browser and a video viewing application, the applications that share ML models can be any type of application, e.g., shopping applications, media applications, games, etc. Personalization in this manner can improve the user experience of using apps. The described techniques are implemented with specific user permission and in compliance with applicable regulations.

Further to the descriptions above, a user is provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user’s activity in an application, a user’s preferences, personalized ranking models), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot
be determined. Thus, the user may have control over what information is collected about the
user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques to securely provide a machine learning model (or
other types of predictive model) trained on user activity in a particular app to one or more other
apps on the same device. The model can then be used on the same device by the other apps to
generate personalized rankings or recommendations for the user, without having access to user
activity data. Personalization in this manner can improve the user experience of using apps. The
described techniques are implemented with specific user permission and in compliance with
applicable regulations.