

System and Method for Protecting Sensitive Production Data for Machine Learning Model Generation

Abstract

In a described embodiment, a request associated with a generation of a machine learning model in a development environment is received, wherein the machine learning model includes a plurality of source code. A set of metadata associated with a real dataset of a production environment based on the request is read and the set of metadata for populating a synthetic dataset is transmitted to the development environment. The synthetic dataset in the development environment for training the machine learning model is processed and the source code of a trained machine learning model is scanned to determine source code vulnerabilities. The source code vulnerabilities corresponding to the trained machine learning model are corrected and after the correction, deployment of the trained machine learning model as a validated development model to the production environment is achieved.

Figure 1