Creating explainable, ethical AI models

Trustworthiness hinges on being be able to communicate how algorithms make predictions



Rohit Dhanda Vice President of Federal, H2O.ai

RTIFICIAL INTELLIGENCE IS an essential component of IT modernization. It enables agencies to make sense of their data, which leads to more informed decisions about how to achieve the goals of modernization: improving processes, operations and the customer experience.

Machine learning models can be built to increase efficiencies, such as cost controls and predictive maintenance. They can be built to make data more actionable so that agencies can improve responsiveness to constituents, enhance situational awareness for warfighters and mitigate cybersecurity risks. Models can also be built to increase the government's accountability in terms of mission effectiveness, taxpayer benefits, compliance with regulations, and reduction of fraud, waste and abuse.

Following standards for responsible AI

The outcome of an AI model should be properly explained and communicated, and agencies must follow ethical standards for responsible AI. The Defense Department's recent memo on AI spells out the importance of ensuring that the technology is traceable, governable and reliable, which maps to our core tenets at H2O.ai.

Fortunately, the industry continues to make advances in the interpretability of increasingly complex machine learning models. There are many methods and tools that enable users to automatically create documentation to explain how a model works, identify biased data and detect changes in important elements, such as data drift. By enhancing operational transparency and oversight, agencies can ensure that they're using ethical AI.

Leveraging AI on a broader scale

At H2O.ai, we want to make it easier for government agencies to adopt AI. Our platform optimizes operations, mitigates risk such as cyberthreats and provides transparency so that the outcome of an AI model can be properly explained and communicated. Through our partnership with NVIDIA, we use the company's cutting-edge GPUs to speed performance and boost our ability to handle larger datasets.

We also developed the H2O AI AppStore as a platform

for sharing machine learning models that target a range of applications. Analysts who are not necessarily data scientists can use models that have already been built, whether by H2O.ai or by the agency, to start making decisions in no-code and low-code environments. If they want additional capabilities, they can turn to data scientists to build custom models.

It's a huge opportunity to help agencies start leveraging AI on a broader scale in the best way possible. ■

Rohit Dhanda is vice president of federal at H2O.ai.

