

Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11)

Manish Kumar Yadav, SAP

Reducing the Risk of Synthetic Content

E.O. 14110 Section 4.5(a)

Solution: Labeling synthetic content often requires a combination of automated tools and human expertise. Several tools and methods are available for labeling content, including synthetic content. Here are some commonly used tools and approaches:

1. Content Authenticity Initiative: is a coalition of technology companies, media organizations, and academic institutions that aims to develop an open standard for provenance and verification in digital media. The CAI proposes to embed metadata in digital media files that contain details about the provenance of the content, such as the source, creation process, ownership, and distribution.
2. Usage of blockchain for verification, such as metadata, watermarks, and digital signatures.
3. Provenance: it allows organizations to track the origin and history of data, ensuring its quality and integrity.

Advance Responsible Global Technical Standards for AI Development

E.O. 14110 Section 11(b)

Problem: *Best practices for AI model training;*

Solution:

1. Understand problem statement and goals on what we are trying to achieve with ML deployment.
2. Collect concise data and have quality dataset and which is relevant to the problem
3. Start with small set of datasets to understand the model behaviors and then fine tune the hyperparameter and other factor to adjust the result accordingly.
4. Have big set of data to qualify any successful model which gives model confidence.
5. Model versioning: Keep the track of trained model and put a version to track the progress and if it requires to rollback or future training.