Project Internship: Nathan Liénard- Telecom

Title: ModelMatch Plugin: Ensuring LLM Compliance with Pre-Defined

With the growing use of Large Language Models (LLMs), ensuring that used models online meet predefined specifications is essential. ModelMatch is a plugin designed to verify that users is really interacting with the exact LLM they requested. By performing a pre-check, the plugin ensures that the used model aligns with expected parameters such as size, structure, and metadata, helping users maintain consistency in their workflows. LLM offered in sofwtare-as-a-service may not always match the requested specifications. Furthermore, users may also unintentionally download models (locally on their machine) that have been altered, quantized, or configured differently, leading to variations in expected performance.

Additionally, changes in file sizes may indicate the use of unintended versions, such as quantized models instead of full-sized ones, impacting model accuracy and efficiency.

Objectives:

- Study what are the important parameters that impact the output of LLM models and can be be differentiated through the use of the LLM them with a good accuracy
- Do a state-of-the art analysis of APIs used to access LLMs
- Evaluate the difference of outputs for a LLM and its variant
- Develop a plugin that verifies the correctness of a LLM through its API

Steps:

- Definition and state of art : study the list of parameters to be pre-checked (according to which parameters)
- Prototype Development: Build the initial version of the ModelMatch plugin with core verification functionalities.
- Testing + Validation: Conduct extensive testing on different LLMs to ensure accuracy and reliability.