Spam Detection: Traditional Machine Learning and Deep Learning Approaches

The spam detection constitutes a one of the most persistent problems faced by the e-mail security scenario and requires sturdy methods to be able to pinpoint and block unsolicited or malicious messages. With time, from classical Machine Learning and Deep Learning models have been employed for this purpose, each having its advantages depending on the problem under consideration and the working conditions.

Classical ML algorithms like Naïve Bayes, Support Vector Machines (SVM), and Random Forests typically operate on pre-processed, structured features. Such models are trained on the bases of inputs manually engineered to capture his indicators that may include word frequency counts, presence or absence of certain keywords, scores of sender reputation, or attributes of email headers. One very important point to consider about traditional ML models is that they offer transparency and are computationally efficient. In addition, they use less computational power, are easier to debug, and provide explanations for their predictions. For this reason, quite a few traditional methods constitute first-level spam filters in environments where computing power runs low or explainability is required, such as in regulated areas like finance or healthcare.

Nevertheless, traditional techniques cannot adapt to the increasing sophistication of phishing and spam attacks of modern-day. Modern spam mails could probably undertake adversarial steps, including image obfuscation, or use very natural-sounding language so as to avert rule-based and keyword-based filters. Given that traditional approaches depend so much on manual feature selection, one can argue that.