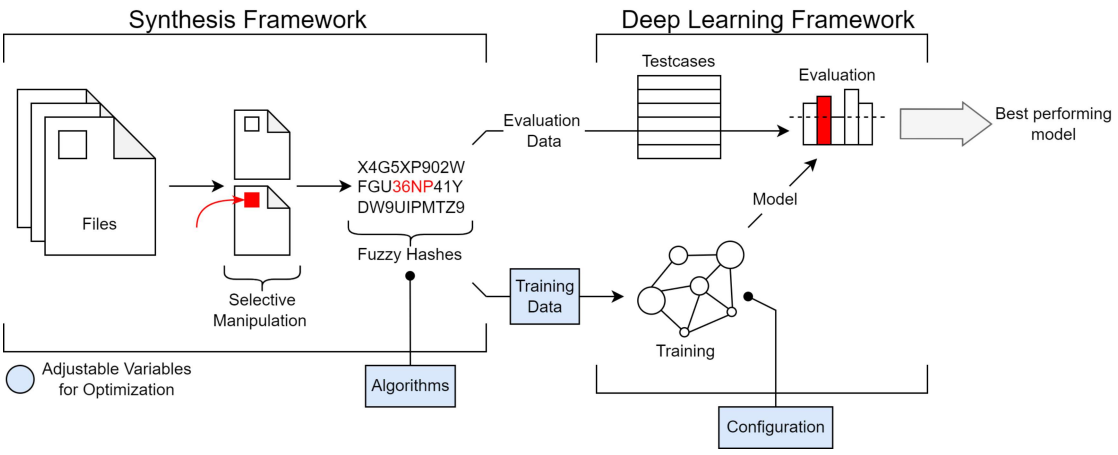

Figure 2.5: Through the choice of the fuzzy hash, training data and configuration, the evaluation performance of the deep learning assisted approximate matching models can be optimized on a quantitative basis.

I argue that the current literature reflects two research gaps: First, a need for a comprehensive evaluation framework that evaluates current byte-wise approximate matching algorithms with synthetic data. Second, a need for the understanding of the merits of deep learning-assisted approximate matching in another context than malware detection.

Evaluating a neural network on adjustable synthetic data would provide the perfect ground truth to understand further the benefits of applying deep learning onto fuzzy hashes. Figure 2.5 shows an example of how a synthesis framework and a deep learning framework could aid in exploring and optimizing future models.

In the spirit of explainable Ai, the strengths and weaknesses of deep-learning assisted approximate matching can be understood by selectively adjusting the input data for the models. As Amarasinghe et al. [2] explained in their work on explainable deep neural network-based anomaly detection, the explanation for detected anomalies is crucial as it improves human operators' trust in the algorithm. When applying anomaly detection onto approximate matching for fragment detection, we want to know why an anomaly was detected in the synthesized data through a neural network and what the networks confidence is. Turning back to our example from earlier: we would want to know whether the basis for a detected anomaly is due to an intentionally placed commonality or due to unimportant noise. A Framework like the one described by Amarasinghe et al. [2]