

Sligpt: How GPT-4o Outperforms in Data Dependency Analysis on Solidity Smart Contracts

Xiaolei Ren^{1†}, Qiping Wei^{2†}

1, Macau University of Science and Technology 2, The University of Texas at Arlington †: Equal contribution

1. Question

GPT-4o can understand and analyze code but still produce non-sense text (known as **hallucination**). How can it be applied to do data dependency analysis while achieving better performance than traditional engineering tools?

2. Data Dependency Analysis

- It is one of the widely used static analyses to enhance techniques including taint analysis, fuzzing, and symbolic execution.
- A smart contract consists of state variables and functions that use state variables.
- One dependency analysis on smart contracts is essentially to identify the states variables read in branching conditions and the state variables written for each function.

3. Proposal

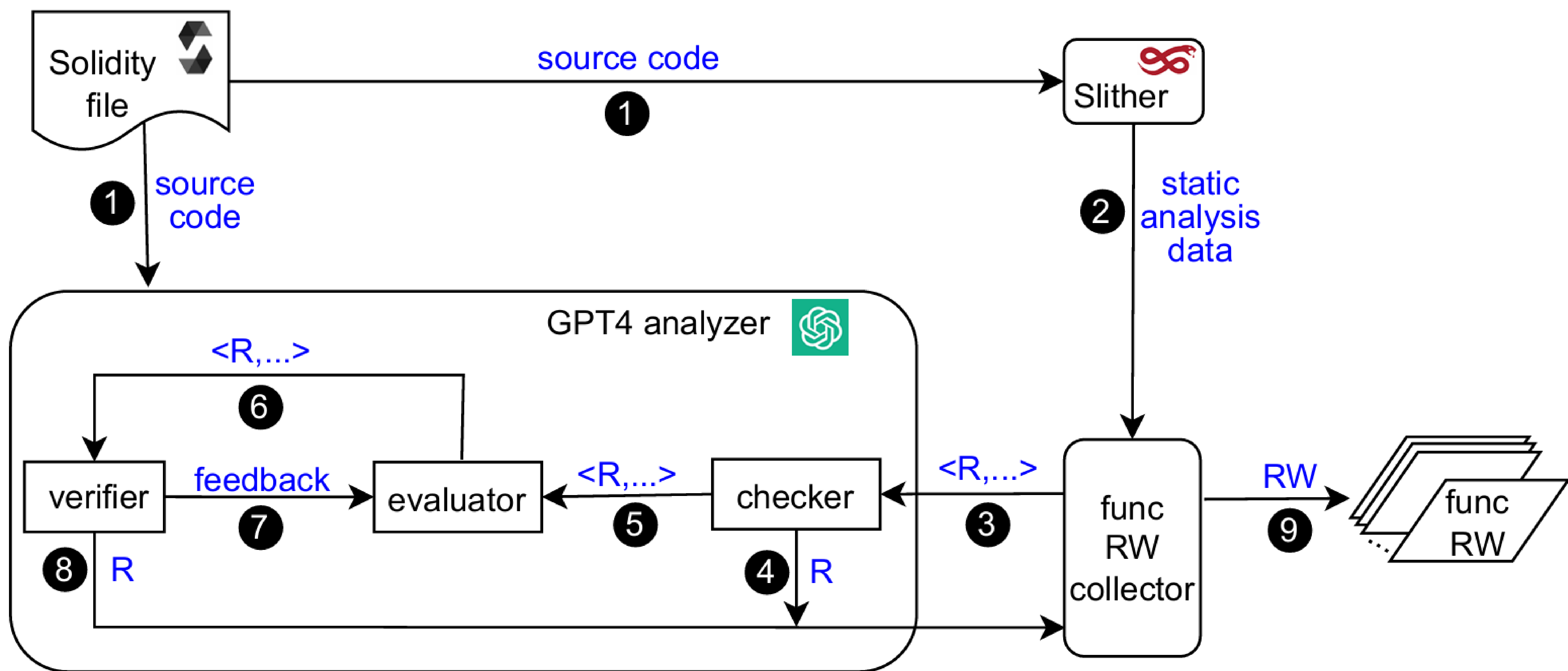
Frame the dependency analysis as the data refining process:

- Provide the initial dependency data.
- Refine the data with **three roles of GPT-4o**:
 - Checker**: examine if the data of a function need to be refined.
 - Evaluator**: either accept the given data or update the data.
 - Verifier**: either accept the given data or provide feedback.

4. How to Reduce Hallucination

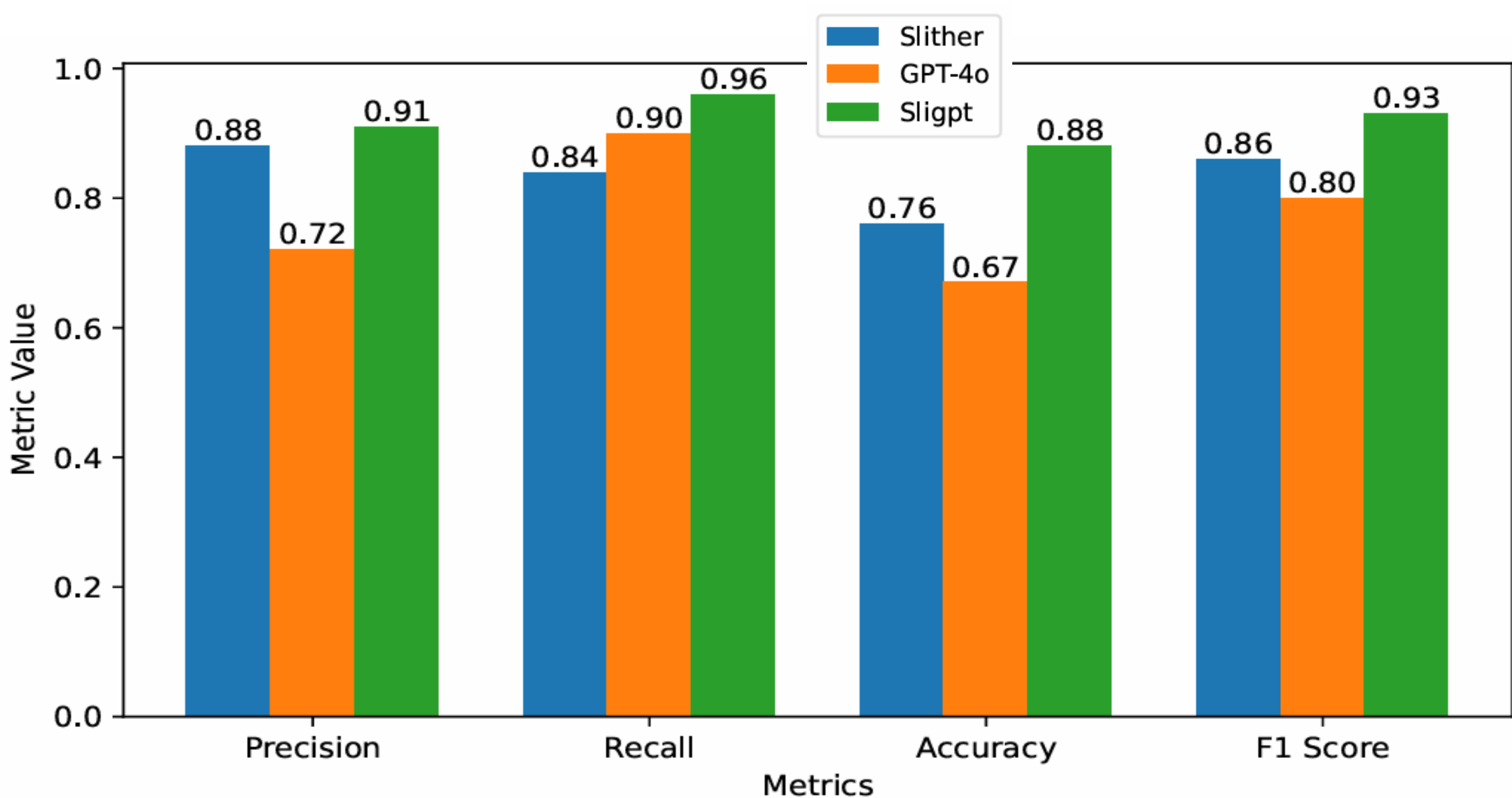
- Not generate the dependency data directly.
- Design to refine the dependency data.
- Minimize the data to be refined.
- Provide more context information to GPT-4o.

5. Architecture of Sligpt



R: the reads of state variables in branching conditions in a function; **W**: the writes written in a function; ...: other data like state variables;
Note: **W** is not refined as we observed that the **W** in the given data is correct so far. (see the reason in the third point in Section 4.)

6. Experimental Results



Compared with **Slither** (a popular, well-maintained static analysis tool) and **GPT-4o** (directly generate dependency data), **Sligpt** achieves better results in terms of the four metrics shown above.

7. Conclusion

- Propose a framework Sligpt to perform data dependency analysis.
- Sligpt introduces three roles from GPT-4o to refine the collected dependency data from Slither.
- Experiments show that Sligpt outperforms Slither and GPT-4o.

8. Novelty and Contributions

- Formulate the dependency analysis as the refining process to take advantage of both GPT-4o and a static analysis tool.
- Design different roles from GPT-4o to refine from different perspectives.
- Showcase an instance of applying GPT-4o to perform an engineering task effectively.