

Peer Review

Review of: "MVD: A Multi-Lingual Software Vulnerability Detection Framework"

Guru Bhandari¹

1. School of Economics, Innovation, and Technology, Campus Kristiania, Oslo, Norway

The paper "MVD: A Multi-Lingual Software Vulnerability Detection Framework" introduces an innovative framework designed to detect software vulnerabilities across multiple programming languages. This approach addresses limitations in traditional learning-based methods that are typically restricted to single languages like C/C++, which is insufficient for modern polyglot software systems. While the paper presents a novel and promising approach to MVD, several aspects can be further improved to strengthen the quality.

- The paper focuses heavily on curated datasets for evaluation, which may not accurately reflect the complexity and variability of real-world software projects. The absence of a thorough assessment of diverse, real-world codebases limits the generalizability of the results. The author could present at least one different dataset and real-world data.

- The framework's reliance on CodeBERT, a pre-trained language model, raises questions about its adaptability to languages or coding paradigms not well-represented in the original CodeSearchNet dataset. The model may inherit biases or limitations inherent in CodeBERT, potentially affecting performance in less common or emerging languages. Additionally, it would be interesting to see how it performs with other CLMs (code language models), like CodeLlama, CodeT5+, and so on, or even with newer generic LLMs (at least with one more).

- Although incremental learning is touted as a strength, the paper acknowledges performance variability when adding new languages. This suggests the model's adaptability might be inconsistent, especially when integrating languages with significantly different syntax or semantics from those previously trained.

- The FOLA loss function is introduced to tackle class imbalance, but the paper does not compare this approach against more traditional methods like oversampling, undersampling, or ensemble techniques. It remains unclear whether FOLA offers a substantial improvement over these established methods.
- The model's scalability to handle a broader range of programming languages beyond the six tested remains uncertain. The computational cost of extending the model to numerous languages and maintaining performance is not thoroughly discussed.
- While the paper provides a high-level overview of the framework, it lacks in-depth technical details on the architecture, hyperparameter tuning, and training processes. This makes it harder to reproduce and evaluate the implementation.

In conclusion, while the MVD framework represents an innovative step towards multi-lingual vulnerability detection, its real-world applicability, adaptability to diverse languages, and methodological rigor require further validation and exploration.

Declarations

Potential competing interests: No potential competing interests to declare.