Submission Summary

Conference Name
2025 IEEE International Conference on Acoustics, Speech and Signal Processing

Track Name
ICASSP 2025 Main Tracks

Paper ID
4304

Paper Title
RefleXGen:The unexamined code is not worth using

Abstract
Security in code generation remains a pivotal challenge when applying large language models (LLMs). This paper introduces RefleXGen, an innovative method that significantly enhances code security by integrating Retrieval-Augmented Generation (RAG) techniques with guided self-reflection mechanisms inherent in LLMs. Unlike traditional approaches that rely on fine-tuning LLMs or developing specialized secure code datasets—processes that can be resource-intensive—RefleXGen iteratively optimizes the code generation process through self-assessment and reflection without the need for extensive resources. Within this framework, the model continuously accumulates and refines its knowledge base, thereby progressively improving the security of the generated code. Experimental results demonstrate that RefleXGen substantially enhances code security across multiple models, achieving a 13.6% improvement with GPT-3.5 Turbo, a 6.7% improvement with GPT-4o, a 4.5% improvement with CodeQwen, and a 5.8% improvement with Gemini.

Created
2024/9/9 10:10:49

Last Modified
2024/9/13 13:07:35

Authors
Bin Wang (Peking University) <2201111747@stu.pku.edu.cn>
HUI LI (Peking University) <lih64@pkusz.edu.cn>
Aofan Liu (Peking University) <af.liu@stu.pku.edu.cn>
BoTao Yang (Peking University) <renrulongky999@gmail.com>
Ao Yang (Peking University) <jarvisya@stu.pku.edu.cn>
YiLu Zhong (Peking University) <tangaaang@gmail.com>
Weixiang Huang (China Mobile Internet Co.) <huangweixiang@cmic.chinamobile.com>
Runhuai Huang (State Cloud, Chinatelecom) <huangrh@chinatelecom.cn>
Weimin Zeng (State Cloud, Chinatelecom) <zengwm@chinatelecom.cn>
Yanping Zhang (China Mobile Internet Co.) <zhangyanping@cmic.chinamobile.com>

Primary Subject Area

Information Forensics and Security -> 6.14: Applications and other topics in forensics and security

Secondary Subject Areas

Applied Signal Processing Systems -> 1.14: Applications of generative AI and foundation models

Domain Conflicts

pku.edu.cn;chinamobile.com;chinatelecom.cn

Conflicts of Interest

Aofan Liu - af.liu@stu.pku.edu.cn

- a co-author

Bin Wang - 2201111747@stu.pku.edu.cn

- a co-author

Submission Files

Bin-Wang.pdf (1.3 Mb, 2024/9/13 13:07:17)

Submission Questions Response

1. IEEE Privacy Policy

Acceptance of IEEE Policies are required to register for this event.
By submitting your registration details, you acknowledge that:
You have read and are in agreement with IEEE's Privacy Policy.
https://www.ieee.org/security-privacy.html

Agreement accepted

2. IEEE Event Terms and Conditions

You have read and are in agreement with IEEE's Event Terms and Conditions.
https://www.ieee.org/conferences/event-terms-and-conditions.html

Agreement accepted

3. IEEE Code of Ethics

You have read and are in agreement with the IEEE Code of Ethics.
https://www.ieee.org/about/corporate/governance/p7-8.html

Agreement accepted

4. Signal Processing Society Opt-In

I would like to receive information about conferences and other opportunities from the Signal Processing Society that may be of interest to me.

Agreement accepted

5. Author Order

I confirm that the author order on the PDF paper matches the author listing submitted to CMT.

Agreement accepted

6. ORCID ID

Enter the ORCID ID of the corresponding author, if available. Please edit your CMT user profile and include it there as well.

[Not Answered]

7. Author Status

Please indicate your author status.

STUDENT

8. NOTE: Author Status

Please fill out the information below for your co-authors. ICASSP 2025 will use these details to contact eligible co-authors and offer them the opportunity to sign up as reviewers if they are interested.

We are limiting the below fields to the first five authors, but additional authors can be listed on the paper.

Agreement accepted

9. Author #2 Email

Author #2 Email

[Not Answered]

10. Author #2 Status

Author #2 Status

[Not Answered]

11. Author #3 Email

Author #3 Email

[Not Answered]

12. Author #3 Status

Author #3 Status

[Not Answered]

13. Author #4 Email

Author #4 Email

[Not Answered]

14. Author #4 Status

Author #4 Status

[Not Answered]

15. Author #5 Email

Author #5 Email

[Not Answered]

16. Author #5 Status

Author #5 Status

[Not Answered]