Lecture Notes on Data Engineering and Communications Technologies
Volume 242, 2025, Pages 53–65

Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method

Adamantis, M.[a], Sokolov, V.[a], Skladannyi, P.[a]

[a]Borys Grinchenko Kyiv University, Ukraine

Abstract

Proactive detection of vulnerabilities in smart contracts is imperative for ensuring the security of user funds entrusted to them. Once deployed, a smart contract is immutable and therefore cannot be updated. This posits the challenge of detecting and fixing all vulnerabilities before deployment. In this context, static analysis has proved to be a formidable tool, even though there is still a lot to be discovered in this field, and the likelihood of the discovery of new classes of vulnerabilities is high. Since 2019, there has been a rise in methods that use Machine (ML) and Deep Learning (DL) to enhance the existing methods, whether in static or dynamic analysis, to cover this issue. This research presents a comprehensive review of existing ML models that detect vulnerabilities in smart contracts statically, i.e. without running their code. The authors evaluate the accuracy of publicly available models in identifying reentrancy in smart contracts based on their F1 score when tested on a foreign dataset with files of newer Solidity versions. The findings point to the limitations of such models in adapting to the continuously evolving nature of the Solidity language, which is still going through its infancy. The authors also explore and share the optimal parameters for training and testing those models, detailing things that were overlooked by the official documentation. All the scripts used for integration and interoperability were published on GitHub to facilitate further research in this area. The research highlights the critical need for constantly updating the existing detectors to avoid false negatives. This research is significant for the broader blockchain community, safeguarding smart contract integrity and fortifying overall system security. © The Author(s), under exclusive license to Springer Nature Switzerland AG.

Author keywords

Blockchain security; Decentralized finance; Machine learning; Smart contracts; Static analysis; Vulnerability detection

About this paper

https://link.springer.com/chapter/10.1007/978-3-031-84228-3_5

ISSN: 2367-4512
DOI: 10.1007/978-3-031-84228-3_5
EID: 2-s2.0-105002775622

Source Type: Book Series
Document Type: Book Chapter
Publisher: Springer, Cham