A Study on Adapting Software Engineering Techniques to New Testing Context with Data-Driven Approach

葉, 家鳴

https://hdl.handle.net/2324/7157360

出版情報：Kyushu University, 2023, 博士（工学）, 課程博士
バージョン：
権利関係：

（様式 2）

氏　　名　：葉　家鳴

論 文 名　：A Study on Adapting Software Engineering Techniques to New Testing Context with Data-Driven Approach
(データ駆動型アプローチによる新たなテスト環境へのソフトウェア工学技術の適応研究)

区　　分　：甲

論 文 内 容 の 要 旨

The software testing phase plays a critical role in the software development lifecycle, but it is often time-consuming, accounting for approximately 50¥% of the project's time budget. While software testing aims to verify software compliance with requirements, the adaptiveness of existing testing approaches remains a significant challenge. As software applications become more specific to particular domains, adapting existing techniques to new testing contexts poses difficulties due to domain knowledge requirements, differing test criteria, and technical implementation challenges. This thesis focuses on adapting existing approaches in two new testing contexts: GUI testing and smart contract testing. The research is conducted through three key steps:

1. Data-Driven GUI Testing: Leveraging the advancements in AI techniques, the thesis explores the application of data-driven methods in GUI testing. Object detection models are proposed to detect GUI widgets and aid in generating test scripts. A dataset is created using game GUIs for training models, and different models are evaluated for their detection precision. The results show that the trained models achieve a precision of 52.9¥% and a recall 59.1¥% on the testing dataset. Challenges in GUI detection, such as compactly placed GUIs and style variety, are also identified and discussed.
2. Smart Contract Testing and Vulnerability Detection: The thesis investigates the domain knowledge required for smart contracts, particularly about vulnerabilities that pose security threats. Vulnerability detection tools for smart contracts are evaluated, and based on their findings, the thesis summarizes four vulnerable signatures and six benign signatures. A vulnerability detector called Vulpedia is implemented, outperforming other tools in terms of precision and recall in vulnerability detection. Vulpedia also exhibits superior efficiency, requiring only 883 minutes to detect vulnerabilities compared to the 8,859 minutes needed by Securify.
3. Data-Driven Smart Contract Testing: The thesis addresses the oversight of cross-contract vulnerabilities in existing smart contract testing tools. To improve the efficiency of detecting cross-contract vulnerabilities, data-driven approaches are proposed to guide fuzzing testing. A vulnerability dataset is collected and used to train models, achieving a remarkable recall rate of 95¥% and minimal vulnerability misses. The proposed tool, xFuzz, outperforms other tools by identifying 18 cross-contract vulnerabilities, with 15 of them being missed by existing tools. Additionally, xFuzz detects twice as many vulnerabilities as other tools less than 20¥% of the time.

In summary, this thesis contributes to adapting existing GUI and smart contract testing approaches in two

novel testing contexts. The research demonstrates the effectiveness of data-driven methods in GUI testing, addresses the domain gap in smart contract testing through vulnerability detection, and proposes data-driven approaches to detect cross-contract vulnerabilities efficiently. The findings and tools presented in this thesis offer valuable contributions to enhancing software testing practices in evolving application domains.