Quality Assessment of ChatGPT Generated Code and their Use by Developers

Mohammed Latif Siddiq
msiddiq3@nd.edu
University of Notre Dame
Notre Dame, IN, USA

Jiahao Zhang∗
jzhang38@nd.edu
University of Notre Dame
Notre Dame, IN, USA

Lindsay Roney
lroney@nd.edu
University of Notre Dame
Notre Dame, IN, USA

Joanna C. S. Santos
joannacss@nd.edu
University of Notre Dame
Notre Dame, IN, USA

ABSTRACT
The release of large language models (LLMs) like ChatGPT has revolutionized software development. Prior works explored ChatGPT’s generated response quality, the effectiveness of different prompting techniques, its performance in programming contests, etc. However, there is limited information regarding the practical usage of ChatGPT by software developers. This data mining challenge focuses on DevGPT, a curated dataset of developer-ChatGPT conversations encompassing prompts with ChatGPT’s responses, including code snippets. Our paper leverages this dataset to investigate (RQ1) whether ChatGPT generates Python & Java code with quality issues; (RQ2) whether ChatGPT-generated code is merged into a repository, and, if it does, to what extent developers change them; and (RQ3) what are the main use cases for ChatGPT besides code generation. We found that ChatGPT-generated code suffers from using undefined/unused variables and improper documentation. They also have security issues related to improper resources and exception management. Our results show that ChatGPT-generated codes are hardly merged, and they are significantly modified before merging. Based on an analysis of developers’ discussions and the developer-ChatGPT chats, we found that developers use ChatGPT for every stage of software development and leverage it to learn about new frameworks and development kits.

CCS CONCEPTS
• Software and its engineering → Software performance; Software usability; Empirical software validation.

J. Zhang was a visiting student at ND from SUSTech (Southern University of Science and Technology) when this research was performed.

±Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

MSR ’24, April 15–16, 2024, Lisbon, Portugal
© 2024 Copyright held by the owner/authors(s). Publication rights licensed to ACM.
ACM ISBN 978-8-4007-0587-8/24/04 $15.00
https://doi.org/10.1145/3643991.3645071

1 INTRODUCTION
The release of GitHub Copilot [15] and ChatGPT [2], two code generation assistants based on Large Language Models (LLMs), is reshaping software development [26]. A recent survey [29] showed that 92% of 500 US-based developers are using LLM-based code generation tools for both work and personal use. Code generation models help developers automate repetitive tasks, focusing on higher-level, challenging tasks [44].

Although these code generation assistants are increasingly popular among developers [44], prior studies have shown that they can generate code that contains quality issues, such as code smells, security smells, and vulnerabilities [24, 35]. A recent study [31] also showed that code generation tools are fine-tuned with samples containing code/security smells that leak to the generated code. With the increasing use of LLM-based code assistants, these problematic code snippets can get deployed into production, negatively affecting the software system’s security and reliability.

Although there are studies about code generation models [24, 31], there is no study about chat-style multimodel, i.e., ChatGPT [2]. As developers can make conversations about software development that are not limited to traditional code generation, ChatGPT can provide answers to developers in every step of software development (e.g., software management, testing, deployment etc.). Moreover, there is no study about the ChatGPT-generated code from the perspective of code quality issues mined from real developers’ prompts.
Thus, we investigate the quality issues of ChatGPT-generated code and their influence on developers’ discussions. We used the DevGPT dataset [43] to investigate the code and security smells in the generated Python and Java code using three static analyzers, Pylint [4], Bandit [1] and CodeQL [16]. We also investigated if the ChatGPT-generated code merged into the code base. Furthermore, we did an open coding of the discussion and conversations in the pull requests where developers posted ChatGPT share links.

Our work provides the first view of quality issues in the code generated by ChatGPT and how the code is used among software developers. Our result shows that ChatGPT-generated codes have issues using undefined and unused variables and no proper documentation. They also suffer from improper resources, exceptions, and cryptography security management and use hard-coded credentials. Our result also shows that most ChatGPT-generated codes are not merged from the pull requests. Developers use the conversation to learn about libraries, frameworks, refactoring, and debugging code. The replication package can be found online [32, 33].

2 BACKGROUND AND RELATED WORK

2.1 LLM-based Code Generation

LLM-based code generation techniques produce source code from a given prompt. A prompt can be a combination of natural language and source code. The code generation problem can be treated as a sequence-to-sequence (seq2seq) learning problem [36] and prior works used Recurrent Neural Networks (RNN) and neural networks based on Long Short-Term Memory (LSTM) [30, 36] to generate source code. More recently, the attention-based transformer architecture revolutionized the field of language learning [41]. There are several transformer-based deep learning models that are fine-tuned with code-related datasets for source code generation [17, 19, 37], search [10], and summarization [13]. Examples of this model type include CodeBERT [10], CodeT5 [42], and Codex [7]. ChatGPT [2] is optimized for conversation and can also generate code.

2.2 Code Smell

A code smell (“bad code smell” or “smell”) is an indicator of an improper choice of system design and implementation strategy [11, 12]. These flaws can stifle software development or increase the chance of future errors or failures [25]. An example of a smell token from Siddiq et al. [31] is using the wrong exception catching order, as shown in Figure 1. The `Exception` block is never reached, as the `Exception` block will catch all exceptions.

![Code smell example](image)

**Figure 1:** Examples of a code smell and a security smell

Security code smells (or simply “security smells”) are a subset of code smells. They are common code patterns that may lead to security flaws [27, 28, 31]. Although security smells may not be a vulnerability per se, they are symptoms that signal the prospect of a vulnerability [14]. For example, the code snippet in Figure 1 has a security smell related to the use of hard-coded credentials (CWE-798) [31]. This code snippet checks the password to a hardcoded string (i.e., “password!”), which can be exploited using a list of commonly used passwords.

Code and security smells introduce quality issues and negatively affect a project’s maintainability, readability, and security [12]. As manually identifying smells is time-consuming and may not scale [20], several works [6, 18, 23] developed techniques to detect code smells. Lanza and Marinescu [20] proposed a metric-based detection strategy to detect code smells, while Chen et al. [8] implemented a code smell detection tool, PySMEll, which can detect 11 code smells in a Python project. Di Nucci et al. [9] described machine learning-based experiments with a new dataset configuration that includes instances of multiple types of smells.

2.3 Empirical Studies on Code LLMs

Prior works investigated the usability of code generation models [39], whether they can generate vulnerable code [24] or whether it is as bad as humans in generating insecure code [5]. Siddiq et al. [31] focused on quality issues in the code generation datasets and their leakage from the closed and open source models. In other projects, they created a dataset and framework to systematically evaluate generated code from the security perspective [34, 35]. Liu et al. [21] focused on the quality issues of ChatGPT-generated code, but they are limited to programming problems from LeetCode [3]. Unlike these prior studies, we study real prompts made by software developers who used ChatGPT to generate code.

3 METHODOLOGY

In this study, we answer three research questions:

**RQ1 Does ChatGPT generate code with smells?**

A recent study [31] showed that datasets used to train open-source LLMs contain code and security smells that leak to the output generated by these models. In this RQ, we investigate whether ChatGPT, a closed-source LLM, also generates code with quality issues, i.e., containing code smells and security smells.

**RQ2 Are ChatGPT-generated source codes merged into open source projects?**

In this RQ, we investigate whether developers reuse code generated by ChatGPT in merged pull requests. In doing so, we also inspect what type of changes (if any) developers make prior to merging the generated code into production.

**RQ3 How are developers using ChatGPT?**

In this question, we aim to understand the use cases for ChatGPT beyond code generation. We investigate how developers use ChatGPT by analyzing the chat conversations.

To answer these RQs, we use the DevGPT dataset [43]. This dataset contains ChatGPT sharing links found in posts made on HackerNews as well as in code files, commits, issues, pull requests, and discussions posted on GitHub. This dataset has 2,345 share links. Each shared link corresponds to a chat between a developer and ChatGPT. This chat conversation can include not only natural language but also code written in different programming
languages. In this study, we focus on the generation of code written in Python and Java, as these are two popular languages among developers [22]. The next sections describe how we answer each of these RQs.

3.1 RQ1: Smells in Generated Code
To answer RQ1, we retrieved all share links mined from GitHub, i.e., links found in files, commits, issues, pull requests (PRs), or PRs’ discussions. Next, we excluded conversations that did not include code written in Python or Java. This way, we obtained 696 Python files from 357 ChatGPT conversations. Since 52 of these Python files (7.47%) had syntax errors, in the end, we had 644 ChatGPT-generated Python code. In the case of Java, we initially obtained 147 Java files from 69 ChatGPT conversations. We converted them into Maven projects, naming the files according to the public class name, and added dependencies as needed in order to make the code compilable. Yet, not all the generated Java codes could be compiled as some used classes that were not available in the conversation. Once we discarded un compilable samples, in the end, we had a total of 67 Java source codes from 35 ChatGPT conversations. To identify quality issues, we ran Pylint (v3.0.2) [4] and Bandit (v1.7.5) [1] on the Python files and CodeQL (v2.14.6) [16] for the Java files:

- Pylint [4] is a static analyzer for Python that can display five message types: fatal (i.e., unable to process the file), error (i.e., code smells that may lead to runtime errors), warning (i.e., Python-specific smells), convention (i.e., codeviolations stated standards), and refactor (i.e., code smells that can be fixed through refactoring). Similar to a prior study [31], we ignored messages related to style issues about whitespaces, newlines, and invalid names as well as import-related messages as Pylint is not reliable in checking for import statements usage [40]. We also omitted fatal messages.

- Bandit [1] is a static analyzer that detects security smells in Python code. Each detected security smell maps to an ID from the Common Weakness Enumeration (CWE) ID [38].

- CodeQL [16] is a static analyzer that checks for style issues and vulnerabilities in a project by executing QL queries against a database generated from the source code. We used CodeQL to check for issues related to the following categories: Advisory, Architecture, Compatibility, Complexity, Dead Code, Language Abuse, Performance, Violations of Best Practices and Security.

3.2 RQ2: Generated Code in Merged PRs
To answer RQ2, we leveraged the metadata data from pull requests (PRs) where ChatGPT share links were mentioned. We only included PRs whose status was "merged" and that had at least one modified/added Python or Java file, obtaining a total of 50 PRs. We then manually inspect each of these PRs and compare them with the source file(s) in the pull request to identify the files that contain verbatim copies or similar code to the ones generated by ChatGPT.

For each PR, we also note what changes (if any) were made by developers to the generated code before merging it.

3.3 RQ3: ChatGPT Use Cases
In RQ3, we analyzed the developers’ discussion in 39 out of the 50 PRs retrieved in RQ2, along with the chat conversation within the ChatGPT share link. We could not analyze 11 PR discussions as they were not in English or had no discussion texts. During this open coding, we analyzed the pull request’s title, body, and each comment made by the developers where the ChatGPT conversation is mentioned (if it is not mentioned in the PR body). We analyzed the context in order to annotate them with concepts (codes). This coding was performed by one of the authors of this paper, who has a software development experience of 2 years. The open code was then vetted by two other authors with 3 and 10 years of experience each. After reviewing the pull request information, we collaboratively highlighted the key points (see Section 4.3).

4 RESULTS
4.1 RQ1: Generated Code Quality
Table 1 shows the quality issues found by Pylint, Bandit, and Cod- eQL to the Python/Java code generated by ChatGPT. We found that most messages for Python files are error and convention type. The top messages for each category are undefined variables, missing docstrings, too few public methods in a generated class, and redefining a variable declared in the outer scope. ChatGPT-generated code also suffers from security issues. Results from Bandit [1] show that there are 84 security issues and the top three of them are requests without a timeout (CWE-400: Uncontrolled Resource Consumption), using pseudo-random generators (CWE-330: Use of Insufficiently Random Values) and using asserts (CWE-703: Improper Check or Handling of Exceptional Conditions).

For Java code, the issues are about not using proper JavaDoc in public methods, constructors, or variables, dead code, unused maven dependencies, and unused and unread local variables. In terms of security smells, ChatGPT mainly provides hard-coded credentials in the code, which is related to CWE-798: Use of Hard-coded Credentials.

4.2 RQ2: Generated Code in Merged PRs
Out of the 50 analyzed PRs containing ChatGPT share links, only 6 of them (12%) contained generated code that was merged into the repository. Out of these 6 merged codes, 3 of them were verbatim copies of the generated code, whereas the other 3 contained modifications. To make the modification, developers changed the code to make it compatible with their code base. For example, the following code has been generated by ChatGPT, which uses Jira rest API to check permission to create an issue.

```python
if response.status_code == 200:
    permissions = response.json().get('permissions', {})
    create_issue_permission = permissions.get('create_issues', False)
```

The following code, taken from a merged pull request3, uses the example above and is modified for the same purpose.

### 4.3 RQ3: ChatGPT Use Cases

After doing an open coding of PRs’ discussions and the corresponding conversations with ChatGPT, we observed the following use cases for ChatGPT:

- **Libraries & Frameworks**: We found that ChatGPT was used in 36% of cases to get help with the APIs for (1) standard (built-in) Python modules / Java packages and (2) external Python modules / Java APIs. For example, we observed conversations in which developers sought help with Python’s string manipulation methods, datetime module, and deepcopy of objects. ChatGPT’s conversations were also used for understanding public libraries, especially for machine and deep learning frameworks, e.g., Pytorch, TensorFlow, pandas, skrub, pydantic, SparkAI etc.

- **Code Formatting and Refactoring**: We found 6 (15%) chats in which developers used ChatGPT for code formatting and standardization. For example, ChatGPT provided suggestions to a developer on how to re-structure a developer’s Python script into multiple files and folders. In another use case, we found that developers used ChatGPT to obtain advice on how to automatically check type hints in a Python project, to which case ChatGPT suggested using the library mypy.

- **Testing and Deploying**: We found 9 chats (23%) in which ChatGPT provided suggestions to developers related to version controlling, unit & integration testing, dependency management and documentation. Developers also use it to obtain help for deployment frameworks like Jira.

- **SDK Help**: In 4 of the analyzed conversations, ChatGPT was used to understand and troubleshoot software development kits (SDKs). The most commonly mentioned SDKs were Nylas-SDK, AWS SDK for Python (Boto3), and konfuzio-SDK.

- **Debugging**: Although ChatGPT prompts are limited to 4,000 tokens, we found 3 conversations in which developers used ChatGPT to debug file uploading issues, audio conversation problems, and arbitrary code execution.

- **Miscellaneous**: In 8 cases, ChatGPT was also used in miscellaneous use cases such as networking, bioinformatics-related data manipulation, message exchange, and audio streaming.

### 5 DISCUSSION

#### Quality Issues in the Generated Code

Our findings in RQ1 showed that ChatGPT-generated codes have quality issues like not following standard coding practice, need refactoring, and security smells. The generated codes use undefined variables and return data outside of the functions. They are also poorly documented and keep undefined variables and arguments in the method. ChatGPT-generated code also faced security issues like not using timeout in resource-sensitive API calling, providing `assert` without proper exception management, and using hardcoded credentials.

**Implication for the Developers**: Developers are using ChatGPT for various purposes, as our findings in RQ3. They can be used to learn about unfamiliar libraries and development kits. Developers make conversations about code formatting, testing, and deployment. They also can be used for code debugging. However, our results in RQ1 show they are not free from code and security smells. They should be appropriately vetted before using the code base.

#### 5.1 Threats of Validity

In our work, the dataset is used for a mining challenge, DevGPT [43], which can introduce external threats to validity. However, the dataset is vetted by the organizers. Our work focused on Python and Java, two of the top-used programming languages among developers, according to a survey from Stack Overflow [22].

Another validity threat to this work is that we used three static analyzers (Pylint [4], Bandit [1], and CodeQL [16]) to detect code quality issues. They can introduce false positives, but their precision is significantly high according to the literature [24, 31]. Another threat to this work concerns the manual evaluation of the PRs’ discussions and chats. The author’s professional software development experience and the peer review by the other senior authors mitigated this internal validity threat.

### 6 CONCLUSION AND FUTURE WORK

ChatGPT is revitalizing the software development process. Our work shows developers use them for code formatting, debugging, testing, and deployment. They are using it for learning new frameworks. However, the generated code from ChatGPT can be standard and have security smells. Moreover, they can be merged into the software code repositories. In the future, we are going to extend
our work to other programming languages and investigate how the developers interact with ChatGPT to reach the solution.

REFERENCES


