Code at the Speed of AI

Evaluating the Trade-offs Between Productivity and Security

Muhammed Ali Elhasan, Yousef Abbas, Zakaria Aslan

Department of Computer Science

University of Gothenburg

February 26, 2025

Abstract

Generative AI is rapidly transforming software development by enhancing productivity. AI-assisted tools accelerate coding, yet they introduce notable security challenges. This proposal examines the trade-offs between efficiency and potential vulnerabilities. A mixed-methods approach, including surveys and code analyses, will be used to explore these issues. The goal is to offer insights that balance development speed with secure coding practices.

1 Introduction

Generative AI has revolutionized the software development workflow by automating repetitive coding tasks, suggesting solutions, and improving code quality. Tools such as GitHub Copilot and OpenAI's ChatGPT provide real-time code suggestions and debugging assistance, enabling developers to work faster and more efficiently [1]. Research has shown that AI-powered coding assistants significantly improve programmer productivity by reducing development time and minimizing errors [2]. These tools are especially beneficial for early career developers, helping them adapt to industry challenges by lowering barriers to entry and increasing their productivity [2]. This study focuses on how these tools have reshaped software development practices and workflows.

Furthermore, while AI-driven coding tools improve productivity, they also introduce potential security vulnerabilities that can compromise the integrity and reliability of software [3]. Studies have shown that AI-generated code can contain security flaws that developers may not immediately recognize, increasing the risk of exploitation [4]. These risks include the generation of insecure code, exposure to dependency vulnerabilities, and the inclusion of hard-coded credentials. According to a recent report by Snyk, more than 50% companies using AI-generated code encountered security issues, underscoring the need for rigorous validation and security assessments [4].

Additionally, AI models trained on public code repositories may unintentionally replicate vulnerabilities found in their training data, which can increase security risks [5]. It is essential to understand these security implications to ensure that the benefits of AI tools are used effectively while minimising potential risks.

2 Related Work

The integration of generative AI into software development has been extensively studied, particularly concerning its impact on productivity, associated security risks, and developer perceptions. This section reviews existing literature in these areas and identifies research gaps that this study aims to address.

2.1 The Role of Generative AI in Software Development Productivity

Generative AI tools have significantly impacted software development efficiency by automating routine tasks and providing real-time code suggestions. Studies have shown that developers using AI-assisted coding tools experience notable improvements in productivity. Peng et al. (2023) conducted a controlled experiment revealing that developers using GitHub Copilot completed tasks 55.8% faster than those without AI assistance [6]. Similarly, a report by McKinsey (2023) highlighted that AI-powered coding assistants reduce debugging time and improve code accuracy, particularly for early-career developers [7]. However, these studies focus primarily on the advantages of AI tools, without addressing their potential risks.

2.2 Security Risks in AI-Generated Code

Despite the productivity benefits, AI-generated code introduces security risks that could compromise software integrity. Snyk's 2023 report revealed that over 50% of organizations faced security vulnerabilities due to AI-generated code, with common issues including weak encryption practices, dependency risks, and hardcoded credentials [4]. Furthermore, Brown and Williams (2023) analyzed AI model training data and found that public repositories often contain insecure patterns that AI systems reproduce, exacerbating security concerns [5]. While these findings emphasize AI-related security challenges, existing literature lacks a structured framework to mitigate these risks without compromising productivity.

2.3 Developer Perceptions of AI in Software Development

Understanding how developers perceive AI-generated code is critical to evaluating its real-world impact. A survey by DevTech Insights (2023) found that while 85% of developers acknowledged AI's efficiency gains, only 42% fully trusted AI-generated code without manual review [8]. Similarly, recent studies suggest that developers adopt AI assistance differently based on their experience levels, with senior engineers using AI for boilerplate tasks and junior developers relying on it for logic generation [9]. These findings indicate that AI trust issues may limit its effectiveness, warranting further investigation.

2.4 Research Gaps and the Need for Further Study

Existing studies emphasize either the productivity benefits or security vulnerabilities of AI-generated code but do not adequately examine their trade-offs in a structured manner. Additionally, most research focuses on AI's effectiveness rather than real-world security implications in production environments. While some frameworks exist for evaluating secure coding practices, they are not tailored to AI-generated code [10]. This study aims to bridge these gaps by systematically evaluating the benefits and risks of AI-driven development and proposing actionable recommendations for balancing productivity with security.

3 Methodology

This study employs a focused approach to examine the balance between productivity and security in AI-assisted software development.

3.1 Data Collection

- **Developer Survey:** An online survey with 30-40 software developers focusing on AI tool usage patterns, productivity impacts, and security awareness.
- **Code Analysis:** Examination of 20-25 code samples generated by popular AI tools, evaluated for both efficiency and security vulnerabilities.

3.2 Analysis Framework

Quantitative and qualitative analysis of collected data to identify correlations between AI tool usage and both productivity metrics and security outcomes.

4 Research Questions

This study seeks to address the following research questions:

- **RQ1**: How do AI tools impact developer productivity?
- **RQ2**: What security issues emerge in AI-generated code?
- **RQ3**: How to balance efficiency and security with AI tools?

These questions will guide the data collection and analysis processes throughout the study.

References

[1] E. Roshi, "10 best ai tools for developers 2025 (compared)," *Tech AI Magazine*, 2025. [Online]. Available: `https://codeless.co/best-ai-tools-for-developers/`.

[2] R. Ferdiana, "The impact of artificial intelligence on programmer productivity," in *Proceedings of the International Conference on Software Engineering and Information Technology (ICOSEIT)*, 2024. [Online]. Available: `https://www.researchgate.net/publication/378962192_The_Impact_of_Artificial_Intelligence_on_Programmer_Productivity`.

[3] J. Schmitt, "Risks and rewards of generative ai for software development," *CircleCI Blog*, 2024. [Online]. Available: `https://circleci.com/blog/risks-rewards-generative-ai/`.

[4] Snyk, "Ai-generated code leads to security issues for most businesses: Report," *CIO Dive*, 2023. [Online]. Available: `https://www.ciodive.com/news/security-issues-ai-generated-code-snyk/705900/`.

[5] J. Brown and K. Williams, "Ai models trained on public code: A security risk analysis," *Journal of AI and Cybersecurity*, vol. 15, no. 2, pp. 45–60, 2023. [Online]. Available: `https://www.researchgate.net/publication/380192131`.

[6] S. Peng, E. Kalliamvakou, P. Cihon, and M. Demirer, *The impact of ai on developer productivity: Evidence from github copilot*, Feb. 2023. DOI: `10.48550/arXiv.2302.06590`.

[7] McKinsey Company, "The future of ai in software development," *McKinsey Insights*, 2023. [Online]. Available: `https://www.mckinsey.com/`.

[8] DevTech Insights, "Ai adoption in software engineering: Developer perceptions," 2023. [Online]. Available: `https://www.devtech.com/research`.

[9] GitHub, "Survey reveals ai's impact on the developer experience," *GitHub Blog*, 2023. [Online]. Available: `https://github.blog/news-insights/research/survey-reveals-ais-impact-on-the-developer-experience/`.

[10] C. for Security and E. Technology, "Cybersecurity risks of ai-generated code," *CSET Report*, 2023. [Online]. Available: `https://cset.georgetown.edu/publication/cybersecurity-risks-of-ai-generated-code/`.