

---

# SOK: EXPLORING HALLUCINATIONS AND SECURITY RISKS IN AI-ASSISTED SOFTWARE DEVELOPMENT WITH INSIGHTS FOR LLM DEPLOYMENT

---

A PREPRINT

**Ariful Haque**

Department of Cyber Physical Systems  
Clark Atlanta University  
Atlanta, GA, USA  
mohdariful.haque@students.cau.edu

**Sunzida Siddique**

Department of Computer Science and Engineering  
Dhaka International University  
Dhaka, Bangladesh  
sunzida15-9667@diu.edu.bd

**Md. Mahfuzur Rahman**

Silicon Orchard Research and Analytics Lab  
Dhaka, Bangladesh  
mahim@siliconorchard.com

**Ahmed Rafi Hasan**

Department of Computer Science and Engineering  
Dhaka, Bangladesh  
rafihasan@cse.dhaka.edu

**Laxmi Rani Das**

Department of Computer Science and Engineering  
Dhaka, Bangladesh  
laxmi.das@cse.dhaka.edu

**Marufa Kamal**

Department of Computer Science and Engineering  
Dhaka, Bangladesh  
marufa.kamal@cse.dhaka.edu

**Tasnim Masura**

Department of Cyber Physical Systems  
Clark Atlanta University  
Atlanta, GA, USA  
tmasura@students.cau.edu

**Kishor Datta Gupta**

Department of Cyber Physical Systems  
Clark Atlanta University  
Atlanta, GA, USA  
kgupta@cau.edu

## ABSTRACT

The integration of Large Language Models (LLMs) such as GitHub Copilot, ChatGPT, Cursor AI, and Codeium AI into software development has revolutionized the coding landscape, offering significant productivity gains, automation, and enhanced debugging capabilities. These tools have proven invaluable for generating code snippets, refactoring existing code, and providing real-time support to developers. However, their widespread adoption also presents notable challenges, particularly in terms of security vulnerabilities, code quality, and ethical concerns. This paper provides a comprehensive analysis of the benefits and risks associated with AI-powered coding tools, drawing on user feedback, security analyses, and practical use cases. We explore the potential for these tools to replicate insecure coding practices, introduce biases, and generate incorrect or non-sensical code (hallucinations). In addition, we discuss the risks of data leaks, intellectual property violations and the need for robust security measures to mitigate these threats. By comparing the features and performance of these tools, we aim to guide developers in making informed decisions about their use, ensuring that the benefits of AI-assisted coding are maximized while minimizing associated risks.

## 1 Introduction

Large language models have transformed coding by enabling automatic code generation from natural language descriptions. Tools such as ChatGPT, Codium, Copilot, and Cursor AI assist developers in writing, completing,