Sandbox Code Execution System with Integrated AI-Driven Assistance

Naheem M R
Department of Information Science and Engineering HKBK College of Engineering, Bengaluru, India

Adithya V
Department of Information Science and Engineering HKBK College of Engineering, Bengaluru, India

Dhanush H S
Department of Information Science and Engineering HKBK College of Engineering, Bengaluru, India

Harsh Vishwakrama
Department of Information Science and Engineering HKBK College of Engineering, Bengaluru, India

Mohammed Azam
Department of Information Science and Engineering HKBK College of Engineering, Bengaluru, India

Abstract:

This paper presents a secure and scalable online code execution system that leverages Docker containers for robust sandboxing, utilizing Linux control groups (cgroups), namespaces, and seccomp profiles to ensure isolation and security. An AI-driven chatbot, powered by LLaMA 3.2, enhances user learning by providing context-aware programming guidance. User- submitted code is executed in isolated containers, with cgroups enforcing resource limits and seccomp profiles restricting system calls to mitigate threats like fork bombs, infinite loops, and container escape attempts. A Spring Boot backend with WebSocket communica- tion enables real-time interaction, while a PostgreSQL database logs execution metrics and user activity. The AI chatbot analyzes code and terminal output to offer tai- lored debugging and educational support. Performance evaluations show Docker containers achieve startup times of approximately 0.8 seconds, significantly faster than virtual machines (around 12 seconds), with additional advantages in memory, I/O, and energy efficiency. This study explores the system's architecture, security mecha- nisms, AI integration, and performance, highlighting its suitability for educational and competitive programming environments.

Keywords:

Docker, Code Execution System, code isolation, sandboxing.