TU Clausthal

Abschlussvortrag Masterarbeit Shardul Bhatt

„Leveraging LLMs to Address Security Smells in Infrastructure as Code“

In order to develop and update scripts for the development environment, infrastructure, as code is becoming increasingly popular due to technical advancements. In the past, maintenance had to be done manually, which was labour and resource-intensive. Our goal in this research is to examine the detection, generation, and enhancement or improvement in IaC scripts using large language models (GPT models (GPT 4o and GPT o1 Preview)) and Gemini, which has evolved as a trend nowadays. The data has been collected from various sources, like GitHub and StackOverflow. Next, the data was sorted into various security-related smells. Some of the most common security smells are: empty passwords, hard-coded secrets, weak crypto algorithms, using HTTP without TLS, no integrity check, invalid IP binding, suspicious comments, and so on, and then further into different security-related patterns. To assess the capabilities in detection, generation, and improvement, we then used LLMs (GPT models and Gemini) to examine the classified data. The findings demonstrate that, from a security standpoint, GPT models are superior at detection, generation, and enhancing IaC scripts as compared to Gemini. Additionally, the results demonstrate that LLMs efficiency in detecting security smells is enhanced by 42% to 91% in GPT models and by 30% to 63% in Gemini models when prompt engineering is applied.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, Prof. Dr. Jörg P. Müller (Institut für Informatik)
Datum:	Freitag, 28. März 2025, 11:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/sim-uc9-rvy/join