RADIUS

Research in Artificial Intelligence for Development, Innovation and Upgraded Security

Programm / Ausschreibung	KS 24/26, KS 24/26, FH - Forschung für die Wirtschaft 2024	**Status**	laufend
Projektstart	01.01.2025	**Projektende**	31.12.2029
Zeitraum	2025 - 2029	**Projektlaufzeit**	60 Monate
Keywords	AI; LLM; Softwareentwicklung; Security; Nachhaltigkeit		

Projektbeschreibung

Die Revolution der Large Language Models (LLMs) bzw. Generative-AI verändert gerade die Softwareentwicklung in einem Ausmaß, das mit dem Kodak-Nokia Effekt vergleichbar ist. Die heimischen Unternehmen sind aktuell für diesen fundamentalen Umbruch nicht ausreichend gerüstet. Es ist unsere Mission mittels eines niedrigschwelligen Unterstützungsangebots die Betriebe in dieses neue Ära der AI-gestützten Softwareentwicklung und Security zu führen.

Der Schwerpunkt im Einsatz dieser Technologie liegt auf der Code-Generierung, da diese die Produktivität der Entwickler direkt steigert. Dadurch entsteht oft Code von zweifelhafter Qualität und Sicherheit. Die heute existierenden Werkzeuge sind generisch, die Problemstellungen von Unternehmen jedoch spezialisiert. Deren Anpassung an konkrete Problemstellungen ist kostenintensiv. Insbesondere KMU sind bei der Adaption dieser neuen Technologien und Werkzeuge im Nachteil, da es oft an personellen und finanziellen Ressourcen mangelt.

Projekt RADIUS antwortet darauf mit Kompetenz- und Teamaufbau im Themenbereich LLM/Generative-AI, und dessen Anwendung auf Softwareentwicklung bzw. Security, ergänzt durch Use-Cases aus Luftfahrt, Bankenwesen und Embedded Systems-Development. Team-RADIUS wird durch ein universitäres Scientific-Board begleitet und qualitätsgesichert. Es entwickelt Methoden, Best Practices und Trainingsangebote zum Einsatz, Roll-Out und Benchmarking von LLMs bzw. Generative-AI für Softwareengineering und Security. Ergänzt wird dies durch Netzwerkaufbau sowohl mit wissenschaftlichen als auch industriellen Partnern. Ergebnisse werden im Rahmen von wissenschaftlicher bzw. industrieller Dissemination transferiert. Hochschulische bzw. interne Dissemination übertragen diese in die Lehre bzw. zu Schwesterinstituten in den Anwendungsgebieten.

Entscheidender Innovationspunkt ist die Softwareentwicklung und Security mit Generative-AI/LLMs ganzheitlich zu denken. So wird jede einzelne Phase der Softwareentwicklung auf LLM-Einsatz umgestellt, um Software von höchster Qualität und Sicherheit zu erstellen. Im Themenbereich Security gilt dies analog. Eine Bandbreite an Themen von Pentesting bis Intrusion Detection wird durch LLMs unterstützt.

Kernergebnis des Projektes ist ein kompetentes Team, das es Unternehmen, vor allem KMU, ermöglicht den Übergang zu LLM basierter Softwareentwicklung und Security zu meistern. Best Practices, Entwicklungs-Methodik, einfach bedienbare Werkzeuge, Trainings, Dokumentationen, Testszenarien und Pilotprojekte werden aus RADIUS resultierende Artefakte sein. Diese werden sich durch besonders einfache Adaptierbarkeit für KMU auszeichnen.

Projekt RADIUS ist vom bestehenden Josef Ressel Zentrum und den Projekten ENDLESS und FIT4BA klar abgegrenzt. In diesen wird AI-Expertise im Bereich der selbst trainierten AI-Modelle beforscht. Team-RADIUS entwickelt Expertise zu großen vortrainierten Sprach-Modellen. Dies positioniert die FH JOANNEUM zukünftig als umfassende AI Know How Anbieterin.

Abstract

The revolution of Large Language Models (LLMs) and Generative AI is presently transforming software development on a scale comparable to the Kodak-Nokia effect. Currently, regional companies are not sufficiently prepared for this fundamental shift. Our mission is to guide businesses into this new era of AI-driven software development and security through low-threshold support.

The primary focus of this technology's application is on code generation, as it directly enhances the developers' productivity. However, this often results in code of questionable quality and security. The currently available tools are generic, while the problems faced by companies are often specialized. Adapting these tools to specific issues is costly. Small and Medium Enterprises (SMEs) are particularly disadvantaged in adopting these new technologies and tools due to a lack of personnel and financial resources.

Project RADIUS responds to this challenge by building a competent team in the field of LLM/Generative AI and its application in software development and security, complemented by use cases from the aviation, banking, and embedded systems development sectors. Team-RADIUS is accompanied and quality-assured by a university scientific board. It develops methods, best practices, and training offerings for the deployment, rollout, and benchmarking of LLMs and Generative AI for software engineering and security. This is complemented by creating a network with both scientific and industrial partners. The results will be transferred through scientific and industrial dissemination. Academic and internal dissemination will transfer these results into teaching and to neighboring institutes in the areas of application.

A key innovation point is to holistically integrate Generative AI/LLMs into software development and security. Each phase of the software development lifecycle will be adapted to incorporate LLM use, aiming to produce software of the highest quality and security. This approach is analogous in the security domain, where a range of topics from pentesting to intrusion detection will be supported by LLMs.

The core outcome of the project is a competent team that enables companies, especially SMEs, to transition to LLM-based software development and security. Best practices, development methodologies, user-friendly tools, trainings and workshops, documentation, test scenarios, and pilot projects will be artifacts resulting from RADIUS. These will be characterized by their particular ease of adaptation for SMEs.

Project RADIUS is clearly distinct from the existing Josef Ressel Center and the projects ENDLESS and FIT4BA, which researches AI expertise in the area of self-trained AI models. In contrast, Team-RADIUS builds expertise in large pre-trained

language models. This will position FH JOANNEUM as a future provider of comprehensive AI know-how.

Projektpartner

- FH JOANNEUM Gesellschaft mbH