Research Assistant

Faculty IV - Electrical Engineering and Computer Science, Institute of Software Engineering and Theoretical Computer Science / Machine Learning and Security

About us

The Chair of "Machine Learning and Security" at the BIFOLD institute is seeking a research associate (PhD student) for a project within the Excellence Cluster CASA. The project focuses on the security of Large Language Models (LLMs). Its goal is to use differential testing to identify behavioral differences in LLM across model variants, software stacks, and hardware platforms.
The project aims to assess whether these differences affect the security of the models and how the resulting risks can be mitigated.

Your responsibility

- Research and security analysis of LLMs
- Differential testing of LLM implementations
- Development of protection mechanisms for LLMs
- Academic publishing

There is the possibility of pursuing a doctorate.

Your profile

- Successfully completed university degree (Master, Diplom or equivalent) in Computer Science or a related technical field
- Strong knowledge and skills in machine learning
- Strong knowledge and skills in computer security
- Experience with (differential) software testing
- Good knowledge of German and/or English required; willingness to acquire the respective missing language skills
- Ability to work both independently and collaboratively, with a high level of initiative

What we offer

- Exciting and challenging research work
- Collaborative and positive academic environment
- Renowned and dedicated team
- Vivid network of researchers worldwide

How to apply

Please send your application with the **reference number** and the usual documents (one file max. 5
MB) only via email to **hashmi@tu-berlin.de**.

By submitting your application via email you consent to having your data electronically processed and saved. Please note that we do not provide a guaranty for the protection of your personal data when submitted as unprotected file. Please find our data protection notice acc. DSGVO (General Data Protection Regulation) at the TU staff department homepage: https://www.abt2-t.tu-berlin.de/menue/themen_a_z/datenschutzerklaerung/.

To ensure equal opportunities between women and men, applications by women with the required qualifications are explicitly desired. Qualified individuals with disabilities will be favored. The TU Berlin values the diversity of its members and is committed to the goals of equal opportunities. Applications from people of all nationalities and with a migration background are very welcome.

Data protection:

Full job posting:

We've got the brains for the future.
For the benefit of society.