



Technische Universität Berlin



Technische Universität Berlin offers an open position:

Research Assistant - salary grade 13TV-L Berliner Hochschulen

under the reserve that funds are granted; part-time employment may be possible

The new chair of "Machine Learning and Security" headed by Prof. Dr. Konrad Rieck explores the interface between security and artificial intelligence (AI). On the one hand, it develops intelligent systems for the detection of attacks, malware and vulnerabilities. On the other hand, it investigates the security and privacy of learning-based systems. The chair is part of the new AI competence center BIFOLD in Berlin.

The chair is looking for a research assistant (PhD student) to join the DFG project ALISON. The project investigates the security of machine learning in structured domains. In many real-world applications, learning algorithms do not work on vectors but on structured data, such as file formats, natural language or program code. The project explores how attacks on learning algorithms can be constructed with this data and how suitable defenses can be developed.

Fakultät IV -Institut für Softwaretechnik und Theoretische Informatik / FG Maschinelles Lernen und IT-Sicherheit

Reference number: IV-877/22 (starting at the earliest possible / for 3 years / closing date for applications 27/01/23)

Working field:

- Research on the security of learning-based systems
- Development of attacks with structured data (formats, language, code)
- Development of new defense mechanisms
- Scientific publishing and possibility of doctoral studies

Requirements:

- Successfully completed university degree (Master, Diploma or equivalent) in Computer Science or in a related area.
- Strong expertise in machine learning and/or computer security
- Solid knowledge in the area of grammars, parsers and compilers
- Very good written and oral communication skills in English
- Interest and enthusiasm for cutting-edge research
- Creativity and team player skills

Research Environment

- Plenty of exciting and challenging research
- Internationally renowned and dedicated team
- Close cooperation with many research institutions

Please send your written application with the usual documents to **Technische Universität Berlin - Die Präsidentin - Fakultät IV, Institut für Softwaretechnik und Theoretische Informatik, FG Maschinelles Lernen und IT-Sicherheit, Prof. Dr. Konrad Rieck, c/o Sekr. MAR 4-1, Marchstr. 23, 10587 Berlin** or via email to jobs@bifold.berlin.

By submitting your application via email you consent to having your data electronically processed and saved. Please note that we do not provide a guarantee 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/ or quick access 214041.

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.

The vacancy is also available on the internet at <https://www.personalabteilung.tu-berlin.de/menue/jobs/>

