Technische Universität Berlin

Bei der Technischen Universität Berlin ist/sind folgende Stelle/n zu besetzen:

Wiss. Mitarbeiter*in (d/m/w) - Entgeltgruppe 13 TV-L Berliner Hochschulen

Teilzeitbeschäftigung ist ggf. möglich

Die Stelle soll baldmöglichst besetzt werden und ist zunächst bis zum 31.10.2026 befristet.

Das Fachgebiet “Maschinelles Lernen und IT-Sicherheit” beschäftigt sich mit der Schnittstelle zwischen Sicherheit und künstlicher Intelligenz (KI). Es entwickelt neue Ansätze zum Schutz von lernenden Systemen und zur Abwehr von Angriffen und Schadsoftware. Es ist Teil des KI-Kompetenzzentrums BIFOLD in Berlin.
Das Fachgebiet sucht eine:n wissenschaftliche:n Mitarbeiter:in für das Forschungsprojekt AIGENCY. Das Projekt erforscht die Chancen und Risiken von generativer KI (wie LLMs) in der IT-Sicherheit. Es untersucht die Angriffsfläche von generativen KI-Modellen und entwickelt neuartige Angriffs- und Schutzmechanismen. Ziel ist es, Sicherheitsrisiken wissenschaftlich abzuschätzen und frühzeitig einzudämmen. Die Möglichkeit zur Promotion besteht.

Fakultät IV - Institut für Softwaretechnik und Theoretische Informatik / FG Maschinelles Lernen und IT-Sicherheit
Kennziffer: IV-457/24 (besetzbar ab sofort / befristet bis 31.10.2026 / Bewerbungsfristende 13.09.2024)

Aufgabenbeschreibung:

- Erforschung und Sicherheitsanalyse von generativen KI-Modellen
- Analyse von Verwundbarkeiten und Angriffen auf generative KI
- Entwicklung von Schutzmechanismen für generative KI
- Wissenschaftliches Publizieren

Erwartete Qualifikationen:

- Erfolgreich abgeschlossenes wissenschaftliches Hochschulstudium (Master, Diplom oder Äquivalent) in Informatik oder einem ähnlichen technischen Fach
- Sehr gute Kenntnisse und Fähigkeiten im Bereich Maschinelles Lernen
- Sehr gute Kenntnisse und Fähigkeiten im Bereich IT-Sicherheit
- Erfahrung mit der Entwicklung von KI- und/oder Sicherheitssystemen
- Teamfähigkeit, Eigeninitiative und eine selbstständige Arbeitsweise sind wünschenswert
- Gute Deutsch- und/oder Englischkenntnisse erforderlich; Bereitschaft, die jeweils fehlenden Sprachkenntnisse zu erwerben

Forschungsumgebung:

- Spannende und anspruchsvolle Forschung
- Positives und unterstützendes Arbeitsumfeld
- Renommiertes und engagiertes Team
- Internationales Forschungsnetzwerk

Ihre Bewerbung richten Sie bitte unter **Angabe der Kennziffer** mit den üblichen Unterlagen (zusammengefasst in einem PDF-Dokument, nicht größer als 5 MB) **ausschließlich per E-Mail** an **hashmi@tu-berlin.de**.

Mit der Abgabe einer Onlinebewerbung geben Sie als Bewerber*in Ihr Einverständnis, dass Ihre Daten elektronisch verarbeitet und gespeichert werden. Wir weisen darauf hin, dass bei ungeschützter Übersendung Ihrer Bewerbung auf elektronischem Wege keine Gewähr für die Sicherheit übermittelter persönlicher Daten übernommen werden kann. Datenschutzrechtliche Hinweise zur Verarbeitung Ihrer Daten gem. DSGVO finden Sie auf der Webseite der Personalabteilung:
https://www.abt2-t.tu-berlin.de/menue/themen_a_z/datenschutzerklaerung/ oder Direktzugang: 214041.

Zur Wahrung der Chancengleichheit zwischen Frauen und Männern sind Bewerbungen von Frauen mit der jeweiligen Qualifikation ausdrücklich erwünscht. Schwerbehinderte werden bei gleicher Eignung bevorzugt berücksichtigt. Die TU Berlin schätzt die Vielfalt ihrer Mitglieder und verfolgt die Ziele der Chancengleichheit.

Technische Universität Berlin - Die Präsidentin - Fakultät IV, Institut für Softwaretechnik und Theoretische Informatik / FG Maschinelles Lernen und IT-Sicherheit

Die Stellenausschreibung ist auch im Internet abrufbar unter:
https://www.personalabteilung.tu-berlin.de/menue/jobs/

Zertifikat seit 2008
audit familiengerechte hochschule