

Masterarbeit (m/w/d) im Projekt AI-DISCO

Formale Änderungsanalyse zur Neubewertung von Sicherheitsrisiken in Edge-Cloud-Systemen

Im Projekt AI-DISCO untersucht der DFKI-Forschungsbereich Intelligente Netze eine modulare Edge-Cloud-Architektur. Änderungen an Deployment oder Anwendungen können Annahmen über physischen Schutz, Netzwerkzugang oder Vertrauensgrenzen ungültig machen.

Die Forschungsfrage

Wann liefert die Neubewertung nur der direkt oder indirekt von einer Änderung abhängigen Elemente dieselben Annahmenezustände, Risikostufen und erforderlichen Schutzmaßnahmen wie eine vollständige Neubewertung?

Ihre Aufgaben

- Architektur, Deployment-Merkmale und Sicherheitsannahmen als typisierten Graphen modellieren. Annahmen als gültig, ungültig oder unbekannt bewerten.
- Inkrementelles Verfahren entwickeln, das Änderungen über alte und neue Abhängigkeiten verfolgt, und einen Prototyp implementieren.
- Ergebnisgleichheit zur vollständigen Neubewertung formal nachweisen, bei vollständigen Regelabhängigkeiten, deterministischen Regeln und azyklischem Bewertungsgraphen.
- Für industrielle Überwachung und sicherheitskritische Steuerung evaluieren. Ergebnisübereinstimmung, übersehene Auswirkungen, Regelaufrufe und Laufzeit bei Änderungsfolgen messen.

Das bringen Sie mit

- Masterstudium in Informatik, Cybersicherheit oder einem verwandten Fach
- Interesse an IT-Sicherheit, formalen Methoden und Graphalgorithmen sowie Programmiererfahrung
- Selbstständige wissenschaftliche Arbeitsweise und gute Englischkenntnisse

Was Sie erwartet

Individuelle fachliche Betreuung am DFKI und Einblicke in aktuelle Forschung zu sicheren KI-Plattformen. Sie bearbeiten ein abgegrenztes Architekturbeispiel und erarbeiten ein formales Modell, einen Nachweis sowie einen Prototyp mit reproduzierbaren Experimenten.

Interesse an der Masterarbeit?

Senden Sie Ihren Lebenslauf, eine aktuelle Notenübersicht und Ihren frühestmöglichen Starttermin an jan.novacek@dfki.de.

Fachliche Fragen beantwortet Dr. Jan Novacek unter [+49 631 2057 57092](tel:+49631205757092).

Das Deutsche Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) verbindet wissenschaftliche Forschung mit anwendungsnaher Entwicklung im Bereich der Künstlichen Intelligenz.

Wir freuen uns über Interessierte aller Geschlechter und Hintergründe.

Deutsches Forschungszentrum für
Künstliche Intelligenz GmbH (DFKI)
Intelligente Netze
Dr.rer.nat. Jan Novacek

Trippstadter Str. 122
67663 Kaiserslautern
www.dfki.de

[+49 631 2057 57092](tel:+49631205757092)
jan.novacek@dfki.de

Rahmen der Masterarbeit

Geplant: sechs Monate
Beginn nach Vereinbarung

Universitäre Betreuung und formale
Prüfungsfragen sind vor der Anmeldung
abzustimmen.
www.dfki.de