Deadline: **November 2, 2026**

NIAS Complex Systems Programme
School of Natural Sciences & Engineering

National Institute of Advanced Studies (NIAS), Bangalore
Indian Institute of Science Campus, Bengaluru 560 012

Advertisement for Post-Doctoral Associate (RA-III, 1 position) for the DRDO funded project "Novel Methods for Detecting Data Poisoning Attacks on Machine Learning Models"

National Institute of Advanced Studies (NIAS) was conceived and founded in 1988 by the late Mr. J. R. D. Tata, who sought to create an institution to conduct advanced multidisciplinary research. Housed in a picturesque green campus in Bangalore, the Institute serves as a forum to bring together individuals from diverse intellectual backgrounds, in the natural and life sciences, humanities, social sciences, conflict and security studies.

NIAS invites applications from qualified and enthusiastic candidates for the position of Postdoctoral Associate (RA-III, 1 position) to work on a DRDO supported project as described below.

About the Project: Detecting data poisoning in Artificial Intelligence (AI) and Machine Learning (ML) systems (such as Large Language Models or LLMs) is critical to maintaining the reliability, accuracy, and security of deployed models. When attackers manipulate training data, they can subtly alter model behavior, leading to incorrect predictions, biased decisions, or even system failure. Early detection of such threats protects data integrity, preserves user trust, and ensures that AI systems operate safely in high-stakes applications like healthcare, finance, and autonomous systems. This project aims to develop novel defense mechanisms that can be used to defend against various forms of data poisoning attacks on Machine Learning models. It is financially supported by Defence Research & Development Organization (DRDO), Govt. of India, for a period of 3 years.

Position	**Qualification**	**Skills/Expertise**
Post-doctoral Associate (RA-III), One position	Ph.D. (Specialization in Cybersecurity or Computer Science or Machine Learning or related areas) with research experience in Artificial Intelligence/ Machine Learning algorithms and their applications	3 years of post-PhD research experience in the field of computer science with expertise in AI, Machine Learning/ Data science. Publications in peer-reviewed international Scopus indexed journals in Machine Learning algorithms and their applications are highly desirable. ***Expertise in Python programming is a must.***

Tenure: Initial appointment will be for a period of 1 year which will be extended depending on performance and needs of the project.

Emoluments:
Post-doctoral Associate (RA-III): Basic fellowship of **INR 67,000 + HRA**

For details of research of the Principal Investigator, please visit:
URL: https://sites.google.com/site/nithinnagaraj2/

Mode of Application:

Interested applicants should submit their curriculum vitae electronically (as a single PDF document) along with the following documents:-

1. Covering letter (with latest CV)
2. Statement of Purpose (< 2 pages long indicating how the candidate is suitable for the project)
3. Copy of PhD degree certificate
4. PDF copies of at least two publications/writing samples
5. Name, address, and email ID of two referees

The deadline for receiving applications is **November 2, 2026**. Short-listed candidates will be invited for presentation and interview (online mode).

The applications should be addressed to (with subject line 'NIAS-DRDO project position'):

Prof. Nithin Nagaraj
Head, NIAS Complex Systems Programme
National Institute of Advanced Studies (NIAS)
Indian Institute of Science Campus
Bangalore-560, 012, India
E-mail: nithin@nias.res.in