The ***Security Privacy & Trustworthiness in AI*** (SPriNT-AI) lab led by Dr. Karthik Nandakumar at Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI) is looking for outstanding candidates to fill fully funded postdoctoral Research Fellow positions. The openings are immediate, with a flexible start date, and the positions will remain open until filled. The selected candidate will work on a subset of the following topics:

- Adversarial attacks and defense mechanisms
- Robust, secure, and privacy-preserving federated learning
- Learning on encrypted data
- Fairness in machine learning
- Explainable AI
- Biometric recognition and presentation attack detection
- Anomaly detection in surveillance videos

MBZUAI in Abu Dhabi, United Arab Emirates is the world's first university devoted to AI. It is a graduate-level, research-based academic institution that offers specialized degree programs in the fields of machine learning, computer vision, and natural language processing. The University is currently in an ambitious expansion phase aiming to be a world leader in AI within the next five years. The University has approximately 150 Masters and PhD students focusing on topics that cover the complete AI lifecycle. Abu Dhabi offers the perfect balance between megacity-convenience and a small-town liberal setting.

The **SPriNT-AI Lab** at MBZUAI has the mission of developing secure, privacy-preserving, and trustworthy machine learning algorithms. The objective is to conduct research that addresses various trust-related issues in machine learning. **Dr. Karthik Nandakumar** is an Associate Professor in the Computer Vision department at MBZUAI. Prior to that, he worked in the industry for more than a decade as a Research Staff Member at IBM Research and a Research Scientist at Institute for Infocomm Research. He is a Senior Area Editor of IEEE Transactions on Information Forensics and Security (T-IFS) and received the 2019 Outstanding Editorial Board Member award. He is also an Associate Editor for Pattern Recognition journal and a Distinguished Industry Speaker for the IEEE Signal Processing Society.

Work Responsibilities:

- Design, develop, and test novel ideas related to trustworthiness of machine learning systems
- Publish cutting-edge results at top-quality journals (TPAMI, TIFS, TIP, IJCV, CVIU) and conferences (CVPR, NeurIPS, CCS, ICLR, ICML, ICCV, ECCV, AAAI, IJCAI, and KDD)
- Assist with writing research/grant proposals to seek external funding opportunities with government agencies and industry

- Assist in the development of teaching materials for core machine learning/ computer vision courses as well as new courses related to ML security
- Mentor and guide Masters, PhD students, and Research Assistants

Required Qualifications:

- PhD in Computer Science, Electrical Engineering or related field
- Solid background in computer vision and machine learning
- Good programming experience with Python/C/C++ and PyTorch/Tensorflow
- Good written and spoken communication skills
- Good publication record

Key Benefits:

- Attractive salary with supplementary benefits and no tax
- Initial contract will be for a period of 1 year, with possible further extension based on performance
- Opportunity to work in a young and rapidly growing research-focused University and an ambitious research group
- State-of-the-art computing facilities including large GPU clusters
- Opportunities for collaboration with other world-class institutions such as Weizmann Institute of Science
- MBZUAI is located within the Masdar City Free Zone, one of the world's most sustainable urban developments, with great opportunities and support for entrepreneurial activities

Interested applicants should email their CV directly to Dr. Karthik Nandakumar (karthik.nandakumar@mbzuai.ac.ae). Shortlisted candidates will be requested to submit other supporting documents at a later stage.