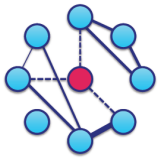
Two PhD Students in the Distributed Systems Group

Privacy-Aware and Adversarial Learning in Big Data Processing

Delft University of Technology, the Netherlands



Delft University of Technology invites applicants for two PhD positions in the Distributed Systems Group in the Department Software Technology of the Faculty of Electrical Engineering, Mathematics and Computer Science.

The Distributed Systems Group

The Distributed Systems group (http://www.ds.ewi.tudelft.nl), under the leadership of Prof. Dick Epema, performs world-class research in the design, implementation, deployment, and analysis of large-scale, Internet-based computer systems. It currently has three research lines: scheduling and resource management in distributed computing systems (e.g., in clusters and clouds), big-data analytics (e.g., differential approximate processing), and cooperative systems (blockchain technology, trust and reputation systems). Its research is fundamental, aimed at the development and evaluation of new generic concepts in systems software, and application-driven, motivated by important application areas. Much of it is experimental, validating the proposed new concepts by means of implementation and deployment in prototypes that are used in the real world.

The Department Software Technology

The Department of Software Technology (ST) is one of the leading Dutch departments in research and academic education in computer science, employing over 150 people. The department ST is responsible for a large part of the curriculum of the bachelor's and master's programmes in Computer Science as well as the master's programme in Embedded Systems. The inspiration for its research topics is largely derived from technical ICT problems in industry and society related to large-scale distributed processing, embedded systems, programming productivity, and web-based information analysis.

The Faculty Electrical Engineering, Mathematics and Computer Science

The Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS) is known worldwide for its high academic quality and the social relevance of its research programmes. Offering an international environment, the faculty has more than 1100 employees (including about 400 PhD students) and more than 2100 bachelor's and master's students. Together they work on a broad range of technical innovations in the fields of electrical sustainable energy, microelectronics, intelligent systems, software technology, and applied mathematics.

Job description 1: Private Learning

The rapid development of AI and big data technology is reshaping our society. While they advance us in the era of digital humanity, several issues and challenges arise, especially relate to data privacy. The key question here is which data set shall be included to construct accurate AI and machine learning models without violating privacy measurements. Moreover, if only a subset of data shall be selected, at which stage of learning shall be executed? In this project, we aim to address this challenge in two fronts: (i) deriving theoretical learning models that guarantee different privacy measurements, e.g., differential privacy, and (ii) developing system prototype that translates the theoretical results into practical software, e.g., Google Rapport.

Job description 2: Adversarial Learning

Artificial Intelligence (AI) and Machine Learning (ML) are ubiquitous in our daily lives, e.g., search engines, machine translation, and self-driving cars. Recent results show that small changes in the input data can alter ML prediction outcomes drastically. The counter-effective examples of AI highlight the importance of building robustness in learning algorithms against malicious adversaries that may intentionally manipulate society. In this PhD project, we aim to explore theoretical and system techniques in the broad area of adversarial learning, where machine learning meets the security research. Examples include studying generative adversary network (GAN) and homomorphic computing, and executing learning algorithms in secure environments, such as intel SGX. The expected outcomes are running ML systems that can withstand a range of adversarial attacks, ranging from data pollution to side channel attacks.

Requirements

We are looking for candidates who satisfy the following requirements:

- an MSc degree with excellent results in Computer Science and Mathematics, preferably in distributed systems, theory, or related areas
- experience in writing python code and system level code, and in conducting scientific evaluations through experimentation
- good speaking and writing skills in English

Conditions of employment

The TU Delft offers a customisable compensation package, a discount for health insurance and sport memberships, and a monthly work costs contribution. Flexible work schedules can be arranged. An International Children's Centre offers childcare and an international primary school. Dual Career Services offers support to accompanying partners. Salary and benefits are in accordance with the Collective Labour Agreement for Dutch Universities. The gross salary for this position ranges from €2222 to €2840 per month.
As a PhD candidate you will be enrolled in the TU Delft Graduate School. The TU Delft Graduate School provides an inspiring research environment, an excellent team of supervisors, academic staff and a mentor, and a Doctoral Education Programme aimed at developing your transferable, discipline-related and research skills. Please visit http://graduateschool.tudelft.nl/ for more information.

Information and application

For more information about this position, please contact Prof. Dick H.J. Epema, e-mail: D.H.J.Epema@tudelft.nl or Dr. Lydia Y. Chen, e-mail: **lydiaychen@ieee.org**. To apply, please send by e-mail an application letter, a curriculum vitae, transcripts of BSc and MSc degrees, copies of BSc and MSc diplomas, proof of language skills if applicable, and the names of two references by **October 1, 2018** to P.T.M. van den Bergh, Hr-eemcs@tudelft.nl. When applying for this position, please refer to vacancy number **EWI2018-60.**