Open PhD position

We are looking for an enthusiastic and motivated PhD student to work on security and privacy of Machine Learning and Artifical Intelligence and the use of AI to design privacy-preserving systems. The PhD will be part of the Privatics Research Group at INRIA which focuses its activity on privacy protection. Example of recent topics include sanitizing motion sensor data, quantifying privacy leakage, explainable AI, SGX-based privacy-preserving systems, detecting vulnerable IoT devices, contact tracing and location privacy. Visit our Privatics web page for more details on recent research. The phd student will help to lead this research theme by working on privacy-preserving federated learning related to medical data and use cases. The student will be co-supervised by Carole Frindel (CREATIS) and Antoine Boutet (Privatics).

Required qualifications

You have a profound understanding of basic ML techniques and have prior experience using them in non-trivial applications. You also have a good grasp of security and privacy concepts in general. Prior research experience is not an absolute requirement, but is a strong plus. In addition to subject matter expertise, you

- are excited about applying these skills to solve practical problems,
- are eager write code and run experiments to test your ideas, and
- have good oral and written communication skills.

If you are interested in this position, drop a message to Antoine Boutet with your current CV and a description of why you think you are a good fit.