POSTDOCTORAL RESEARCHER POSITION IN SECURITY AND PRIVACY FOR BIG DATA (EURECOM)

Research topic

The recent technology developments enable millions of people to collect and share data on a massive scale. Such data allow to derive relevant information about people through advanced analytics such as statistical analysis or machine learning. The analytical findings can help companies improve their customer services, or hospitals identify patterns based on patients' historical data and come up with early treatments. Unfortunately, this new data collection paradigm raises serious privacy concerns mainly because of the high sensitivity of the collected data. Moreover, end-users are usually even not aware of the collection of their personal information. Therefore, there is a strong need for protecting the systems collecting and processing/mining this large amount of data and keeping these data confidential against unauthorized parties.

The goal of the research project is to design and evaluate customized privacy preserving and security primitives that will on the one hand protect the confidentiality of the data and on the other hand enable data centers to perform data mining or machine learning techniques over the encrypted data. To this end, A first study on the privacy and security challenges associated with Big Data applications leveraging different data mining techniques such as statistical data analysis and/or machine learning will be conducted. We will further investigate privacy preserving variants of some specific data mining techniques while leveraging homomorphic encryption solutions. These operations will be tailored to improve the efficiency of the underlying primitives while not sacrificing their accuracy. Another possible approach is to use secure multiparty computation (SMC) which can be used for the protection of data both at the collection and processing phases. Parties involved in the SMC protocol (such as different hospitals) will be able to perform collaborative machine learning over the entire dataset and retrieve the desired results without revealing any information on their respective datasets (patients' health records, eg.).

Requirements:

The position is available immediately and is for one year and is renewable based on availability of funding and mutual interest. Applicants should hold a doctoral degree in applied cryptography or in a related area and have an adequate experience demonstrated through a strong publication record . Some background in in machine learning is appreciated. The working language in the group is English. The position will be funded by an EU-H2020 project.

Contact:

Applications should be sent via email to melek.onen@eurecom.fr and should include a CV, a list of publications (with the top 3 one highlighted), a short research proposal, and contact information for one or two persons who are willing to give references.