Privacy-Preserving Online Services with Trusted Execution Environments

**Keywords**: Distributed systems, data privacy, trusted execution environments.

Nowadays, a wide variety of online services (e.g., web search engines, location-based services, recommender systems) are being used by billions of users on a daily basis. Key to the success of these services is the personalization of their results, that is returning to each user those results that are closer to her interests. For instance, given a web search query sent by two different users, search engines generally rank differently the search results to best fit each user preferences [2]. The latter preferences are generally computed by relying on user profiles that are learnt from past user queries. However, according to the underlying application, user profiles may contain sensitive information about end users. For instance, in the context of location-based services, user profiles contain user mobility data from which it is easy to infer information such as a user’s home and workplace or even her sexual, religious or political preferences if she regularly visits gay bars, worship places or the head quarter of a political party [1]. However, user profiles, which are widely exploited by online service providers due to their inherent business model based on online advertising, might severely threaten user privacy if they end up into the hands of untrusted services. Recent events have shown that the latter risk of data privacy leakage is becoming a reality due to the massive use of cloud services by online service providers and by end users. Indeed, a 2014 study from Gartner found that 94% of organizations either already are or plan to store their consumer data in the cloud. Another study by the same organization envision that the “Cloud Shift” by 2020 will affect more than $1 Trillion in IT spending1. On the same line, cloud providers are experiencing an exponential growth of their storage capabilities2. Due to their success and to the unprecedented value that can be extracted from the data they store (e.g., financial information, health information, trade secrets, intellectual property) cloud providers are becoming the target of devastating attacks3. Examples of such attacks that took place in 2016 include hospital ransomware, millions of Dropbox account details leaked, other millions of Snapchat accounts compromised to cite a few.

In this context, it becomes urgent to devise mechanisms that allow users to securely access online services without fearing that their data will be leaked out from the cloud platforms where it is being stored and processed. For addressing this challenge, the research community in the past years has been very active in devising mechanisms for accessing online services in a privacy-preserving way (e.g., [3, 5, 4, 6]) or for designing novel secure online services (e.g., [7]). However, while the former make rather far reaching trust assumptions, the latter rely on heavy cryptographic techniques. In practice, none of the existing solution can be transposed to reality as the first group of solutions incurs the risk that the assumptions get broken whilst the second group has typically high resource demands and severely degraded service performance.

The objective of this PhD project is to design novel protocols that aim at eliminating these barriers for the success of privacy-preserving online services. We propose to reduce trust assumptions, while still providing improved performance compared to the state of the art.

Examples of online services that might be considered include: location-based services, search engines, recommender systems, ...

The PhD candidate will have to carry out the following steps:

- Perform an exhaustive related work study in the fields of privacy for online services.
- Study the limitations of the existing solutions in terms of privacy guarantees, trust assumptions and performance.
- Propose novel solutions for privacy-preserving online services using trusted execution environments.
- Assess the proposed solution both theoretically and practically through extensive experimentation.

**References:**


PhD Project Ecosystem

Research lab:
LIRIS laboratory, Lyon, France
http://liris.cnrs.fr/

Research group:
Distributed systems and Information Retrieval group (DRIM)
http://liris.cnrs.fr/drim

Supervisors:
Ben Mokhtar Sonia (CNRS researcher)
Sara Bouchenak (Professor at INSA Lyon)

Supervisors email:
sonia.ben-mokhtar@liris.cnrs.fr
sara.bouchenak@insa-lyon.fr

Scientific competence of the research group:
The PhD will be carried out in the DRIM research group headed by Dr. Sonia Ben Mokhtar. It will be co-supervised by Professor Sara Bouchenak. One of the three research axis of the DRIM research group is security and dependability of distributed systems. The group has strong background on the topic and two major publications in the fields related to the PhD proposal can be found below. This PhD project will be carried out in strong collaboration with the team of Professor Rüdiger Kapitza at TU Braunschwheig and the team of Professor Gaël Thomas at Telecom Sud Paris.

Two major publications of the group in the field:


Background required from the applicant:
A good culture in privacy and distributed systems would be appreciated. Good programming skills.