PhD Candidate offer

Tadorea (www.tadorea.com), in collaboration with the Universidad Politecnica de Madrid - Telecommunications Faculty (http://www.etsit.upm.es/), is currently seeking a PhD candidate to undertake his/her PhD programme in the Cryptography field as applied to aviation and, in particular, as applied to air traffic management (ATM).

Today’s aviation operations utilize a set of large, heterogeneous, widely-distributed systems which are sometimes even composed of isolated sub-systems. These are highly complex and very difficult to model analytically, especially considering the interactions between them. Often, detailed data about these systems is needed to understand and benchmark their performance, set up targets, make policies or even plan shared network resources. In the last decade, access has improved to this type of data as well as the computing infrastructures required to store and perform complex calculations with such data. Some of those calculations are, for instance, machine learning algorithms which have also proven their usefulness. Aviation researchers are implementing solutions based on the latest deep learning techniques (DataScience.aero, 2018).

That said, large datasets are not as available to aviation data researchers compared to data availability in other fields. Data science researchers face challenges related to the diversity of inhomogeneous data sources and the large volume of information to be handled and represented. However, the confidentiality of the datasets has historically been the most difficult barrier to data accessibility as most data owners have refused to provide access to significantly large datasets.

In this proposal, a potential approach is presented through the use of state-of-the-art cryptography techniques in overcoming this barrier. By painting some air traffic management data science problems as cryptography systems, and utilizing novel crypto-based solutions, the confidentiality barrier can be overcome without breaking confidentiality requirements. Private data could be used in ATM procedures and systems.

The selected candidate will join TADOREA’s research and development team in Madrid, Spain. His/her PhD thesis will be supervised by Pr. Dr. Victor A. Villagrá from the Telematics Department at the UPM-ETSIT (http://www.dit.upm.es/~villagra/) who will be driving the research plan in applying state-of-the-art cryptography techniques to overcome data sharing barriers in the aviation sector. The combination of skills from the TADOREA and UPM-ETSIT teams will offer the candidate an ideal environment to develop his/her professional career in an environment with strong ATM-domain expertise and state-of-the-art data science, cybersecurity and privacy-preserving techniques.

The PhD programme is framed under the SESAR-Engage Knowledge Transfer Network (http://engagektn.com/) and co-funded by it. As part of this network, the selected candidate will enjoy unique opportunities to participate in summer schools and conferences with other students and researchers in the field. The candidate will have access to a variety of datasets: from airlines, airports, air navigation service providers to other aviation stakeholders. Talented and highly motivated individuals with a great dose of imagination, problem-solving skills, resourceful and data-driven passion are encouraged to apply.
Scientific goals:

Scientific goal 1 - Data privacy in aviation and ATM and challenges to improvements in procedures and system design

The first scientific goal will be to advance the state-of-the-art in understanding how information sharing, using private datasets, can enable new ATM paradigms in performance assessment, policy and regulation and use of shared resources. Establishing the limitations of current solutions and proposing new systems and procedures shall lead to increased performance of the ATM along several KPAs. This in turn helps justify overhead in investment in research and development. Three different concrete scenarios will be defined corresponding to one different prominent challenge scenario in each line of work. Those scenarios should be representative of the line of work and simultaneously show significant barriers and impact potential.

Scientific goal 2 - Design of cryptographic systems for ATM

The PhD candidate should then identify and design cryptographic systems that provide the functionalities sought after each ATM challenge scenario. The second scientific goal will be achieving a cryptosystem that guarantees accurate and secure computation, performs under a concrete communication infrastructure and improves the ATM performance.

Requirements are as follows:

- A university degree in any of the related fields (Mathematics, Physics, Engineering), provided strong skills in Mathematics can be proven.
- Basic understanding of cryptographic systems goals and design.
- Strong background and experience in programming.
- Experience with extraction, acquisition, preparation of data.
- Fluency in English. Only candidates fluent in English should apply, as the interviews might be carried out in English.
- Above all, a strong motivation in developing skills in privacy-preserving data analytics.

Other skills that may be relevant in the evaluation

- Passion for data science on top of current thinking and trends
- Proficiency in Python 3 and data science toolkits knowledge.
- Familiar with distributed data processing architectures, e.g. Spark
- Knowledge or experience with the air transport field.

Tadorea offers a unique set of benefits:

- Immediate start - Candidates are mandated to start the PhD during Q1 2019. Only available candidates should apply.
- Training, internal and external, on the work-related different technologies.
- Integration in a highly qualified and collaborative international team with innovative thinking and agile working methodology.
- Flexibility and good working conditions.

Gross salary: 22.000€

Interested candidates should send the following information to discovery@tadorea.com:

- An up-to-date and detailed CV in pdf format. References, academic records and proof might be requested afterwards but they are not necessary for initial application.
- A research motivational letter, carefully explaining why she or he is the perfect candidate.
- Sharing any professional Internet presence is highly recommended, such as GitHub and/or Stack Overflow profiles, website-blog, portfolio, LinkedIn account, etc.