<center>**Call for a Postdoc Position**</center>

Postdoc context and objectives:

The Internet of Things at large will foster billions of devices, people and services to interconnect and exchange information and useful data. Pointing at the next 30 years, Internet of Things promises a better communication, better access to services by consumers, cost reduction in business activities and increased well-being in our daily lives with its applications in domains such as Health, Smart Cities, Automotive, M2M, and Smart Grids. As IoT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. They are the two most important limitations for the growth of Internet of Things market. Lack of security and trust for the protection of privacy puts a barrier between service providers and consumers, which can be defined as businesses and end user consumers. This barrier directly affects wide adoption of Internet of Things applications in the consumer lifestyle and business applications. Credible, economical, efficient and effective security and privacy for IoT are required to ensure exact and accurate confidentiality, integrity, authentication, and access control, among others. Certain IoT components that have minimal functionality, limited computational power and storage, and low energy resources, which can sometimes make conventional security and privacy protections difficult to deploy. Such deployments may need to take advantage of new protocols and system designs that are better equipped to operate in resource-limited environments.

PARFAIT European project's main goal is to develop a platform for protecting personal data in Internet of Things applications which will be tested with 3 smart domain use-cases. Another goal of the project is to decrease complexity of integrating and deploying services in today's Internet of Things technology by providing interoperable software libraries and tools. Interoperability, along with security and privacy of personal data, are the two most important limitations for the growth of Internet of Things market. Interoperability increases the complexity of service production processes and the cost of production. On the other hand, lack of security and trust for the protection of privacy puts a barrier between service providers and consumers, which can be defined as businesses and end user consumers. This barrier directly affects wide adoption of Internet of Things applications in the consumer lifestyle and business applications.

The postdoc will have the following missions:

- Technical contributions into cyber security aspects and mainly on Intrusion detection in Internet of things using machine learning techniques
- To follow-up the European project with all project partners
- To collaborate with the lab team and mainly the PhD student involved within the European project

Postdoc contract: 18 to 24 months in the context of the European project PARFAIT.

Postdoc location: Engineering school ISAT and its research laboratory DRIVE located in Nevers, France.

Expected starting date: asap.

Experience appreciable in: IoT, Optimization, Intrusion detection, Machine learning.

Expected Profile: Candidates should own a PhD degree in Computer science.

How to Apply: The following documents are required (CV, Motivation letter, two main publications, and reference letters). Send them as attachments of an email, whose subject will be "Application for Postdoc position University of Bourgogne", which must be addressed to Sidi Mohammed Senouci (sidi-mohammed.senouci@u-bourgogne.fr).