Post-doc position

Content-based document signature for IoT security

The L3i laboratory, in the context of the CHIST-ERA SPIRIT project, has one open post-doc position in computer science, in the specific field of document image analysis and pattern recognition.

Duration: 24 months
Position available from: October 1st, 2017
Salary: 2100 € / month (net)
Place: in the L3i lab at La Rochelle, France
Specialty: Computer Science / Image Processing / Document Analysis / Pattern Recognition

Position Description

The work done by the post-doc will take part in the context of the SPIRIT project funded by the CHIST-ERA program (European Fundings).

As the adoption of digital technologies expands, it becomes vital to build trust and confidence in the integrity of such technology. The SPIRIT project will investigate the proof of concept of employing novel secure and privacy-ensuring techniques in services set-up in the Internet of Things (IoT) environment, aiming to increase the trust of users in IoT-based systems. The proposed system will address distinct issues related to security and privacy, hence, overcoming the lack of user confidence, which inhibits utilization of IoT technology.

The proposed system will integrate three highly novel technology concepts developed independently by the consortium partners. Specifically, a technology, termed ICMetrics, for deriving encryption keys directly from the operating characteristics of digital devices comprising the IoT in order to provide an authentication framework for their operation. This prevents spoofing of such devices compromising users' confidential data, and hence leading to increasing the trust and providence of such devices. This technology has been developed by the Universities of Kent and Essex in the UK.

Another technology, termed a Semantic firewall, is a highly flexible network security system, developed by the University of La Rochelle (ULR) in France. The semantic firewall is able to allow or deny the transmission of data derived from an IoT device according to the information contained within the data and the information gathered about the requester, hence ensuring that access to such data is governed by the access permissions commensurate with the requester.

Thirdly, a technology based on creating a content-based signature of user data /documents, in order to ensure the integrity of sent data upon arrival. This technology has also been developed at the University of La Rochelle but has not yet been employed in the IoT domain.

The integration of these technologies will be demonstrated in use case scenario in an IoT based service. In the demonstrator, data extraction and analysis will also be carried out, in order to produce content and semantic information needed by both the content-based signature and the semantic firewall technologies. This part will be carried out jointly by the University of La Rochelle and the University of Geneva in Switzerland.

This project aims to build upon the highly significant results produced by the partners and to research the challenges of how these technologies can be adapted for IoT environment.

More specifically, the work done by the post-doc will consist in two main objectives: (1) extracting content from IoT device data by analyzing the input IoT device data in order to prepare the data for "processing and semantics extraction"; (2) computing a unique content-based signature to allow authenticating an IoT data object independently of its physical representation.

Hence, this work will consist of two parts: data / document analysis and signature computation. In the first part, an IoT data object will be analyzed in order to obtain a robust description of the object, which is independent of the acquisition mode and source. The different components of the document and their spatial relationships (for images this would be printed text, tables, graphics, stamps, handwritten signature…) will be extracted. The aim is to obtain a stable decomposition and reliable content extraction, which conforms to the requirements of the subsequent security-assuring tasks.

The signature computation method, which is the second part, combines cryptographic hash algorithms and perceptual hash algorithms. The cryptographic signature is based on the robust description of the IoT data object. This allows authenticating any object even if it has been subjected to minor modifications as long as these modifications do not change any part of the semantic content.

Qualifications

Candidates must have a completed PhD and research experience in image processing and analysis or pattern recognition.

General Qualifications

- Mastering at least one programming language (like Java, Python, C/C++...)
- Good teamwork skills
- Good writing skills and proficiency in written and spoken English or French

Applications

Candidates should send a CV and a motivation letter to **mickael.coustaty [at] univ-lr.fr** and **petra.gomez [at] univ-lr.fr**

References

1. S. Eskenazi, P. Gomez-Krämer, and J.-M. Ogier. The Delaunay document layout descriptor. In *ACM International Symposium on Document Engineering (DocEng)*, 2015.
2. S. Eskenazi, P. Gomez-Krämer, and J.-M. Ogier. When document security brings new challenges to document analysis. In *International Workshop on Computational Forensics (IWCF)*, Lecture Notes in Computer Science (LNCS 8915), pages 104-116. Springer, 2015.