PhD Title : Service Oriented Security for Fog Computing (SOS4Fog)

Laboratory: LIRIS – UMR 5205

http://liris.cnrs.fr/

Research team: Service Oriented Computing – Dir : F. Biennier / C. Ghedira

Web Site : https://liris.cnrs.fr/equipes?id=62

Supervisor: Pr. Frédérique BIENNIER – INSA de Lyon

Frederique.biennier@insa-lyon.fr

Web site: https://liris.cnrs.fr/membres/?idn=fbiennie&onglet=publique

Working Language: English or French

Abstract:

The digital transformation involved by the IoT, Mobile computing environment and Cloud technologies relies on opened and agile information Systems, able to compose services and exchange information on demand. Such a Dynamic environment calls for a new contextual and information-driven cyber-security management strategy. Success in achieving any benefit from such ICT investment is directly affected by the trust we may have in this Fog organization. Currently, cybersecurity is based on an analysis of threats and assets limited to specific components and is mostly focused on Corporate Information Systems. This leads to consider Fog Computing protection according to a static and well-identified context. Those (service-oriented) risk assessment and security engineering methodologies introduce countermeasures but that can be bypassed by attackers who take advantage of security breaches provided by trusted but poorly secured IoT devices.

To fit these requirements, this research work challenges new security models to define a consistent and contextualized protection for services and Fog computing environment to fit corporate information system security policy requirements (or end-user personal data security and privacy management when using Fog environment based services). To reach this goal, these models will rely on a multi-layer architecture use to integrate safe IoT artifact in the Information system instead of the poorly secured IoT device. The connection between the IoT device, edge node and their “safe artifact” will use a Security@Runtime vision to compose and orchestrate contextually security services.

More precisely, this thesis aims at

1. organizing a multi-layer architecture in order to provide an artifact-based secured vision of the IoT/edge nodes organization
2. organizing a contextual security policy framework (taking into account both services and data protection) to set a fog platform dependent security policy composition framework (mixing traditional “control-driven” process and the “data driven” visions) to select and weave protection services depending on the platform weakness to reach the required Quality of Protection specification
3. develop a security governance loop to manage the convenient security services orchestration in a models@run.time vision.
This research work should be organized as follow:

- State of the art on service security and Fog computing security
- State of the art on Models@Run.Time methods
- Proposition of a Fog Computing multi-layer security architecture
- Identification of protection policy models and on a policy composition algebra
- Specification of the security mediation service @run.time

Collaborations with on-going and forthcoming projects mixing academic and industrial partnerships are expected.

**References:**


