



SOUTENANCE DE THESE THESIS DEFENSE



Lyes TOUATI

Unité de Recherche : **Laboratoire Heudiasyc, Labex MS2T**

soutiendra sa thèse de **Doctorat** sur le sujet :

**Internet of Things security: towards a robust interaction of
Systems of Systems**

A l'Université de Technologie de Compiègne

Le lundi 21 novembre 2016 à 9h30

Amphi L103 – Centre Pierre Guillaumat

Devant le jury composé de :

- M. BOUABDALLAH Abdelmadjid, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc
- M. CHALLAL Yacine, Professeur associé, Ecole Nationale Supérieure d'Informatique, Laboratoire de Méthodes de Conception des systèmes, Algérie
- M. CHEN Lin, Maître de Conférences, Université de Paris-Sud, Laboratoire de Recherche en Informatique, Orsay
- Mme LAURENT Maryline, Professeur des Universités, Telecom Sud Paris, Département RST, SAMOVAR, Evry
- M. SERHROUCHNI Ahmed, Professeur des Universités, Telecom ParisTech, Laboratoire LTCI, Paris

Abstract :

In this thesis, we deal with security challenges in the Internet of Things. The evolution of the Internet toward an Internet of Things created new challenges relating to the way to secure communications given the new constraints of IoT, namely: resource constrained objects, heterogeneity of network components, the huge size of the network, etc.

Indeed, the Internet evolved from a network of computers and servers toward a huge network connecting billions of smart communicating objects. These objects will be integrated into complex systems and use sensors and actuators to observe and interact with their physical environment.

The security requirements of the interactions between smart objects depend on the context which evolves in time and space. Consequently, the definition of the security policies should be adaptive and context-aware.

In this thesis, we were interested in the problem of access control in IoT relying on Attribute based Encryption (ABE). Indeed, ABE schemes present many advantages in implementing a cryptographic fine-grained access control. However, these schemes raise many implementation challenges because of their complexity and high computation and energy overheads.

To overcome this challenge, we leveraged the heterogeneity of IoT to develop collaborative and distributed versions of ABE schemes. Our solutions reduce remarkably the overhead in terms of energy consumption and computation.

The second limitation of ABE schemes is the absence of efficient attribute/key revocation techniques. We have proposed batch based mechanisms for attribute/key revocation in CP-ABE. We demonstrated the efficiency of the proposed solutions through simulations.

Finally, we have proposed a CP-ABE based solution for the problem of grouping proof. This problem consists of providing the proof that a set of objects are present simultaneously (same time and same location). The propose solution has many applications such as enforcing the security of NFC based payments and the access to sensitive locations.