A Framework for Trustworthy Internet of Things

“The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service” (Vermesan et al., 2011).

Security is one of the major challenges in the Internet of Things (IoT). Although various security-related works have been done for IoT, existing works were only based on the classic network security-aspect. For instance, “Cryptography alone cannot solve protecting information in IoT problem as internally compromised nodes can generate bogus information and still authenticate it using valid cryptographic” (Lize, Jingpei, & Bin, 2014). Further, the centralized solutions are not feasible for IoT since fundamentally, IoT is based on distributed environment. Assuming there can be a central management party to govern the entire environment is not realistic. Hence, IoT requires a feasible distributed trust strategy to overcome the drawback of existing security models.

As justified by (Tormo, Mármol, & Pérez, 2014), applying trust to IoT is no longer about designing and developing individual models, but is about how to provide a pool of models. The system should be able to analyze the runtime context and select the best model for the application scenario.

**Project Objective**
This project aims to investigate the possible security attacks in different architecture layers of IoT environments, and the promising solutions. Further, design a software framework architecture that is capable of leveraging different trust models and capable of performing the best trust model for the situation.


