Security and privacy of internet of things

Abstract: According to the International Data Corporation, the Internet of things (IoT) is experiencing a very strong and fast expansion with 1.5 billion devices currently connected worldwide and an 16.9% estimated growth per year to reach 1.7 trillion in 2020 [1]. IoT is expected to generate a huge number of data, with different sensitivity levels, leading to possible data leakages and privacy violation, in the sense of European regulation regarding personal data protection [2]. This thesis addresses security and privacy issues in Internet of Things (IoT), taking into account the constrained-resources of devices (computation, memory and energy). So far, the security and privacy in IoT have been addressed mostly with regard to low cost security and privacy protocols [2]. Another research track known as secure multi-party computation has not been addressed yet in the IoT context. The idea of secure multi-party computation [4] is to make collaborative computations (e.g. addition, scalar multiplication) among a group of entities without revealing any private information that are used as inputs of the collaborative computations. In the IoT, collaborative computation mechanisms are of particular interest for preserving users’ data privacy when a collective service is targeted and operates based on users’ data values, but some adaptations are needed to overcome the topology constraints, and the strong conditions that entities are trustful. Our objective is to design secure and privacy preserving collaborative mechanisms for the IoT environments. The idea is to propose some privacy preserving statistical computations (mean, maximum, minimum, median..) with the assumption that parties are untrusted. We expect taking advantage of recent progress done in collaborative systems based on asymmetric cryptographic algorithms like homomorphic encryption, and lightweight communications based on error-correcting codes cryptography [5]. Keywords: Cryptography, Secure multi-party computation, Privacy. Publications / Patents: [1] International Data Corporation http://www.idc.com [2] Nguyen, K, Laurent, M., Ouahla, N., Survey on Secure Communication Protocols for the Internet of Things. Ad Hoc Networks Journal, Feb. 2015; DOI: 10.1016/j.adhoc.2015.01.006. [3] Weber, R. H. (2010). Internet of Things–New security and privacy challenges.Computer Law & Security Review, 26(1), 23-30. [4] Du, W., & Atallah, M. J. (2001, September). Secure multi-party computation problems and their applications: a review and open problems. In Proceedings of the 2001 workshop on New security paradigms (pp. 13-22). ACM [5] P. Gaborit et al.r. Low Rank Parity Check Codes and their application in cryptography. Workshop WCC 2013.