Security and Privacy Issues in Modern Distributed Systems

Rohit Ranchal

PhD Candidate

Computer Science

Purdue University, IN, USA

rranchal@purdue.edu

Modern distributed systems comprise of a number of loosely-coupled services, which collaborate, interact and share data to accomplish a task. This paradigm is used in many systems such as Cloud Computing, Service Oriented Architecture, Product Lifecycle Management, Pervasive Healthcare, Digital Supply Chains, Smart Homes etc. A distributed interaction involves multiple parties, where each party generates, shares, uses and interacts with the data. Data owner i.e the party that shares data, has no control and visibility on interactions beyond its trust domain. Parties have to rely on each other to ensure data security and privacy. This leads to loss of control. Existing solutions for point-to-point or client-server paradigms are unsuitable in distributed environment because of the involvement of multiple parties in an interaction. The interactions beyond the trust domain of data owner may share data to unauthorized (untrusted) parties and violate owner’s policies and the owner has no way of knowing if a violation occurred. Such interactions introduce new security challenges of unauthorized disclosure and data leakage that are not present in the traditional systems, where the focus is to ensure point to point security. Despite offering a concentration of resources, these solutions also spawn huge risks for data privacy. A single breach can cause significant loss. The heterogeneity of interacting parties represents a danger of multiple, collaborative threats.

Current approaches for protecting shared data trust the receiving party and rely on the use of service level agreements and legal contracts. Trusting a third party requires taking risks. Basically trust and risk are opposite sides of the same coin. Some enforcement and auditing capabilities are required to increase the level of trust. Thus it is imperative to have better solutions that support end-to-end security and protect data according to its owner's policies. An ideal solution should have following characteristics: it should be independent of trusted third party, gives accurate amount of information to the receiving party and provides ability to interact with unknown (untrusted) parties.