Trustworthy Data Sharing and Management for Collaborative Pervasive Computing Applications

Stephen S. Yau, http://dpse.eas.asu.edu/tdsm

**Problem**

Collaborative Pervasive Computing Applications (CPCA) can greatly improve the investigative capabilities and productivity of scientists and engineers. In CPCA, users need to share and manage their sensitive data with high confidence.

We are developing an innovative approach of trustworthy data sharing and management for CPCA based on the specification and generation, trustworthy discovery, and trustworthy access control of data sharing services.

The users of CPCA can share their data by developing of data sharing services using our specification and generation approaches, manage the access to their data through our trustworthy access control approaches, and locate other users’ data with our trustworthy service discovery approaches.

**Approach and Impact**

**Approach**
- Model, specify and match service semantics with situational information and security policies.
- Develop a secure, lightweight, and robust service discovery approach for pervasive environment.
- Adapt access control decisions based on current context and situation.

**Impact**
- Extends current service semantic ontology with data, situation and security policy ontologies.
- Enables users to control the discovery of their service in pervasive environment.
- Incorporates situation-awareness capability in access control models.

**Functionality-based Service Matchmaking**
- Specifies and selects service semantically.
- Filters out functionality incompatible services.
- Defines functionality compatibility based on the input/output parameters and precondition/result situations.
- Aggregates the semantic similarities of parameters, conditions and attributes.

**Situation-Aware Access Control**
- Specify situation-aware access policies
- Using SA-AC policy specification language
- Register these policies with SA-AC agents
- Generate Service Wrappers
- Generate Service Proxies
- Generate user and organization certificates
- Required for authentication and identity of users
- Deploy and run user applications

**Cluster-based Architecture for Service Discovery**
- Organizes the network into multi-hop destined for clusters with efficient clusterhead selections based on connectivity factors
- Ensures connectivity of clusters by deploying a handshake process for cluster membership maintenance.
- Constructs each cluster to be a local DHT-based p2p network for distributed storage of service indices.
- Uses clusterheads as Service Discovery Agents (SDAs) without compromising the privacy of service providers / requesters.

**Disseminate service discovery messages within a cluster**

**Step 1:** Specify and generate data sharing services

**Step 2:** Trustworthy access control

**Step 3:** Situation-aware access control

**Overall Approach of Trustworthy Shared Data Service Management**