

Trustworthy Data Sharing and Management for Collaborative Pervasive Computing Environments

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

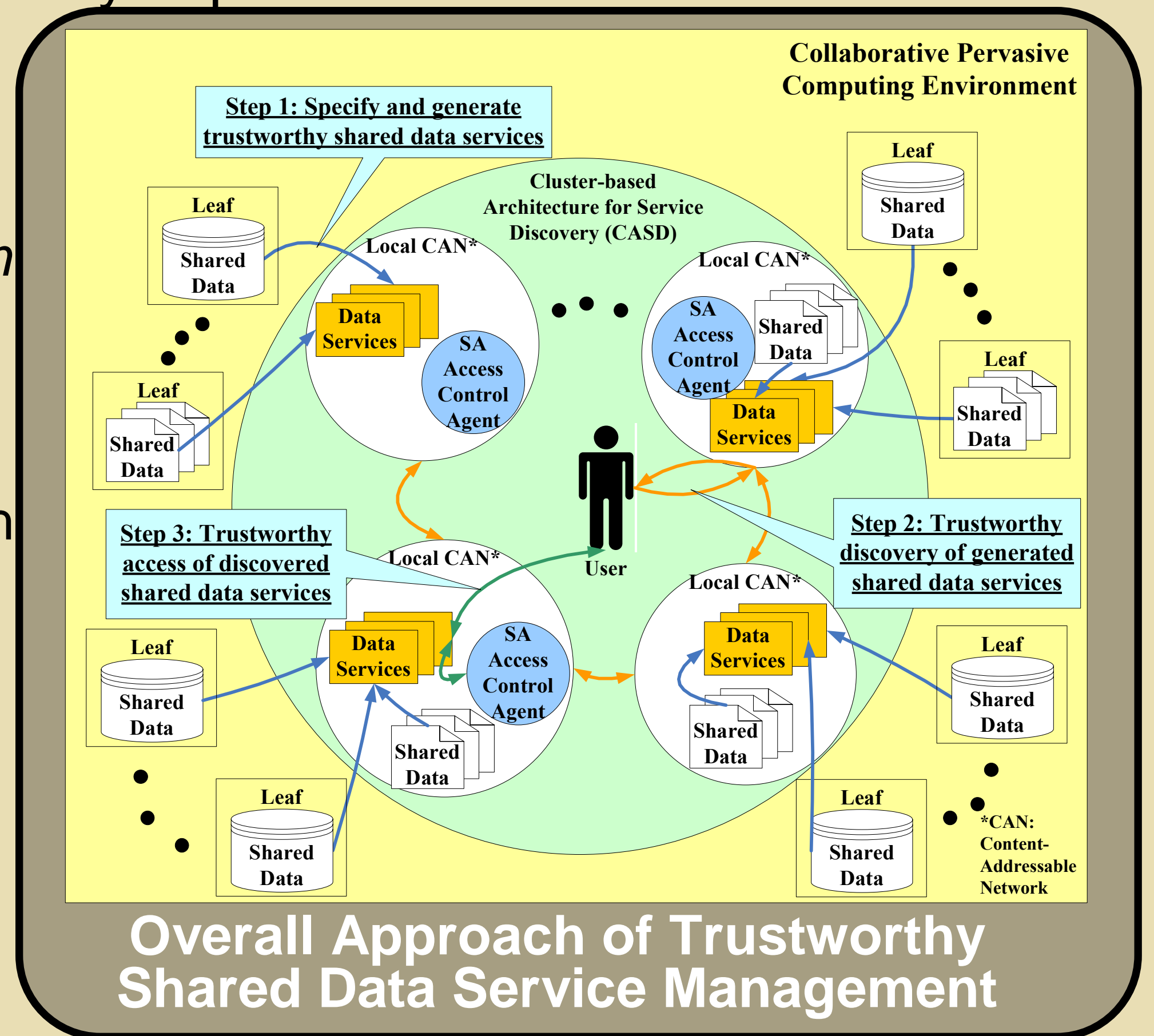


Objective

Collaborative pervasive computing applications (CPCA) can greatly improve the investigative capabilities and productivity of scientists and engineers in many fields. Users of CPCA usually need to share various types of data, including experimental data, sensitive documents, multimedia data, etc. Trustworthiness for data sharing and management in CPCA is a difficult, but very important issue.

In this project, we are developing an innovative approach to enable **trustworthy shared data service management** (including *trustworthy shared data service specification and generation*, *trustworthy shared data service discovery*, and *trustworthy access to shared data services*) to provide CPCA users the capabilities of sharing, discovering and accessing shared data with high confidence.

Demonstration applications will be developed to show that our research results can be easily incorporated in CPCA to increase the trustworthiness and effectiveness of collaborative research or development among scientists, engineers and/or businessmen.



Comparison to the current state of the art

Current state of the art

- Current service specification approaches do not consider semantics of shared data, situation-awareness and related access control policies of the service.
- Existing service discovery approaches for pervasive computing environment only address isolated aspects of trustworthiness
- No systematic way to incorporate and implement flexible access control with situation-awareness.

Our approach

has the following important advantages:

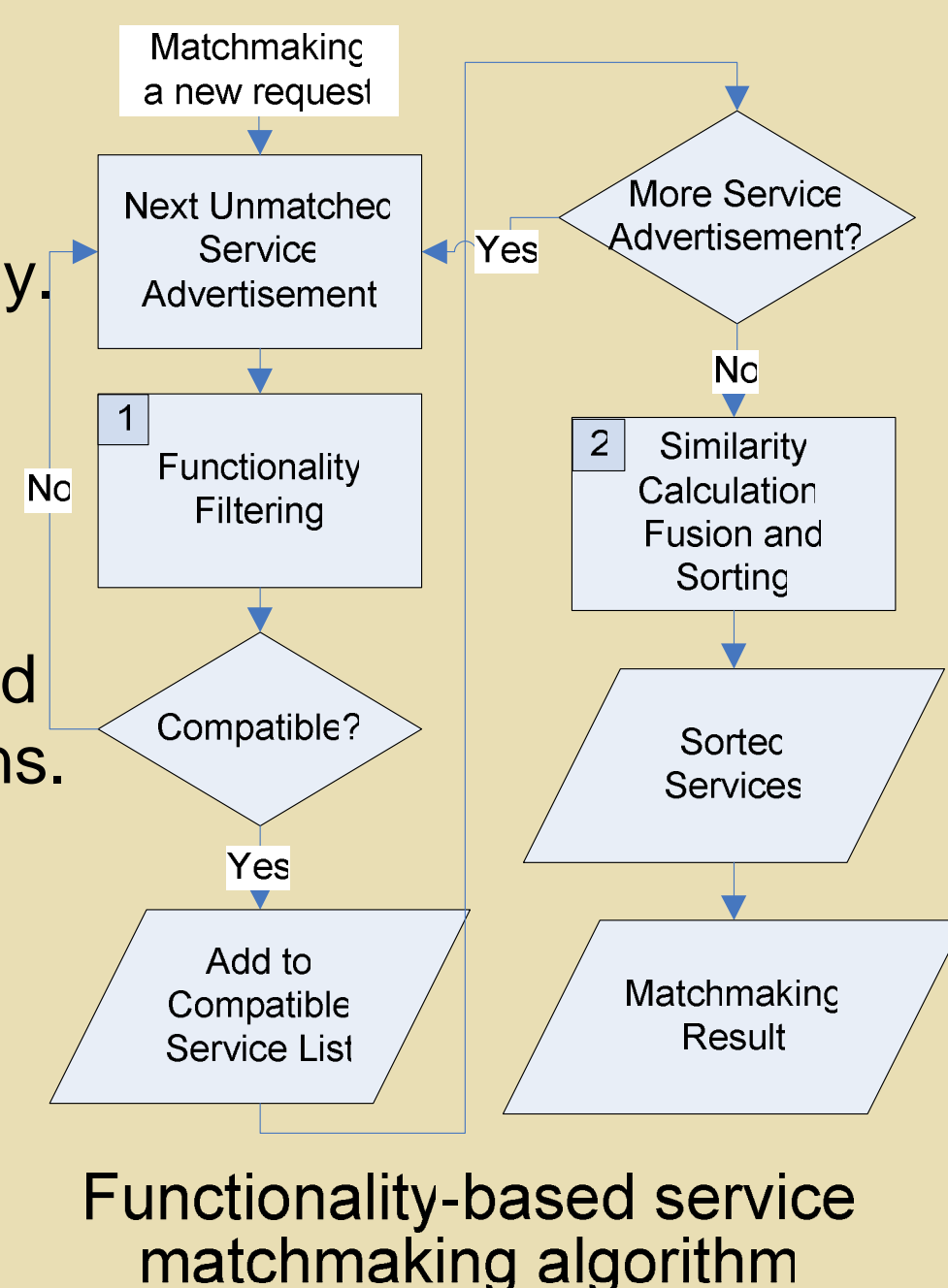
- The *trustworthy shared data service specification* extends OWL-S with data, situation and security policy ontologies.
- The *trustworthy shared data service discovery* addresses the intelligent, secure and anonymous, lightweight, and robust aspects of trustworthiness simultaneously.
- The *trustworthy shared data service access* incorporates situation-awareness capability in access control models.

Current Progress

- Developed a set of **OWL-based ontologies** to specify the semantics of shared data, contexts and situations, shared data services and security policies.
- Developed a **situation-aware access control (SA-AC) technique**, including a SA-AC model, an XML-based SA-AC policy specification language, and a middleware service for reasoning SA-AC policies.
- Developed a **functionality-based matchmaking algorithm** to semantically select services based on their functionalities. Currently, we are incorporating situation-aware service selection in the algorithm.
- Developed a **cluster-based architecture for service discovery (CASD)** to disseminate service discovery messages efficiently. Currently, we are incorporating SA-AC and anonymity preservation into the architecture for more comprehensive trustworthiness.

Functionality-based Service Matchmaking

- 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.



Cluster-based Architecture for Service Discovery

- Organizes the network into multi-hop clusters with efficient clusterhead selections based on nodes' connectivity factors
- Ensures connectivity of the clusters by deploying a specialized handshake process for cluster membership maintenance.
- Constructs each cluster to be a local DHT-based p2p network for distributed storage of service indexes.
- Uses clusterheads as Service Discovery Agents (SDAs) to form a virtual backbone for efficient dissemination of service discovery messages

