

CERIAS

the center for education and research in information assurance and security

Automatic Enforcement of Multiple Policies in Healthcare Domain

Zahid Pervaiz*, David F. Ferraiolo**, Serban Gavrila**, and Arif Ghafoor*

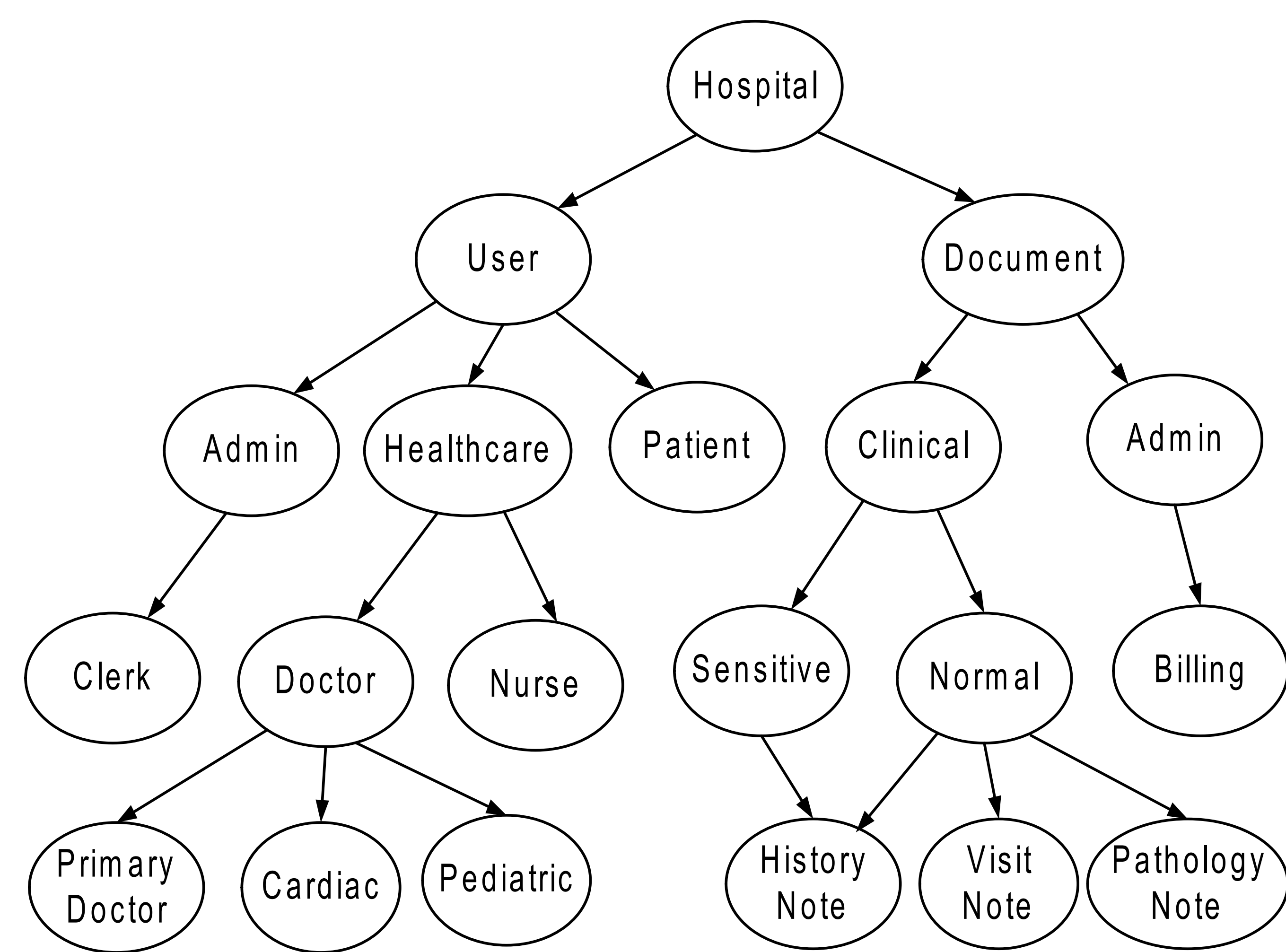
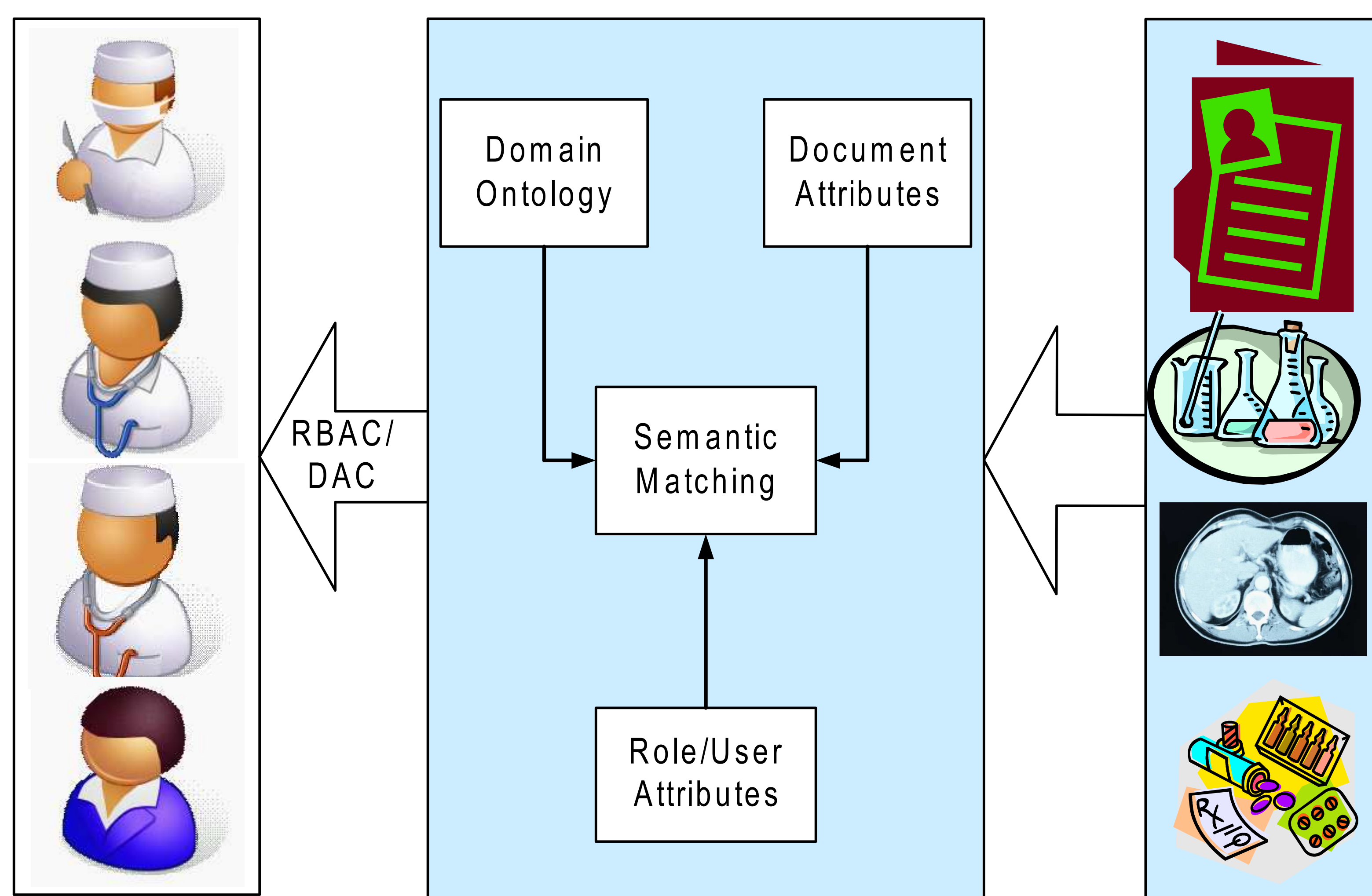
* Electrical and Computer Engineering, Purdue University

** National Institute of Standards and Technology

Objective

Automatic enforcement of

- multiple policies like RBAC and DAC
- based on security rules defined by organisation or user preference
- using semantic matching of domain ontology and object and user attributes



Security Rules:

- Every patient must have access to his/her own health records
- Records declared sensitive should be available to primary doctor only
- Doctor in emergency role can access all health records (sensitive or normal)

Clinical Document Architecture:

- XML markup standard that specifies the structure and semantics of "clinical documents"

Policy Machine(PM):

- Standardized access control mechanism developed by NIST
- Allows enforcement of arbitrary attribute based access control policies
- Enforceable policies may include combination of RBAC, MLS, DAC
- Protection of objects under multiple policies

