This research is underway as a part of the ORF (Ontario Research Fund) project with collaboration of McMaster Department of Radiology, Mohawk College MEDIC lab, and NexJ Health. Currently, the system integration and document sharing among the Diagnostic Imaging Repositories (DI-r) and distributed PACS systems is based on a “Trust Model”, with key challenges such as: lack of federated capabilities to ensure unique user identity in legacy domains; preserving consistency of access control rules across all systems, and monitoring user behavior patterns to enhance security policies. This research introduces a SOA-based architecture (shown below) that provides centralized security among DI-r’s, distributed PACS systems, and mobile clients in the cloud environment, and consists of the following sub-projects [c47]. (b:book; ch:chapter; j:journal; js:journal-submitted; and c:conference)

- Intelligent middleware security provisioning. A secure, central and service-based “intelligent middleware” consisting of: multi-agent technology (smart local agents and administrative middleware agents) for two-level decision-making process; central policy repository and management; central metadata repository for images; and a centralized authentication and decentralized authorization model [j12, js5, js4, c48, c46, c45, c44, c42, c22].
• **Knowledge-driven user behavior-pattern discovery.** This research provides a new generation of intelligent decision support systems that effectively assist the system administrators to obtain deep insight into the system user's dynamic behavior patterns in order to refine the existing security policies using novel approaches to: behavior pattern query language, association and sequential pattern mining, clustering, and visualization [i9, i8].

• **Detecting insider-threats using constrained pattern matching.** This research provides a descriptive language capable of defining a variety of complex user behavior patterns using association, sequencing, and event relationships. A constraint-based pattern matching engine searches the system’s event log repository to discover the instances of the defined behavior pattern that satisfy different hard and soft constraints defined in the behavior pattern. The results will be offered as suggestions and guides that allow the administrators to identify the gaps and flaws in the security policy rules, and the users whose behavior may jeopardize system data integrity.

• **User behavior simulation environment.** An event-log generator engine is developed which receives administrator-defined user-behavior patterns using a pattern language and produces corresponding events in the context of noise events which allows us to effectively test and fine-tune the above techniques before applying them on the production event-logs. Currently we are experimenting with the audit logs from a distributed medical imaging system running at Mohawk College [i11, is6, c49].

• **Enhancing data privacy in service oriented architecture (SOA).** This research enhances data privacy and security, reduces network traffic, and provides new enterprise level features. It introduces two new concepts “task service” and “service representative” in the SOA environment. Task service is a multi-component (model, knowledge, data) web service that can process the client data locally at the client side. Service representative is a generic agent at the client side that will be customized by the knowledge component and will execute the model component on both client and task service data. This approach will enhance the SOA architecture in different ways [j6, js2, js1, c39, c38, c36, c35, c34, c32].