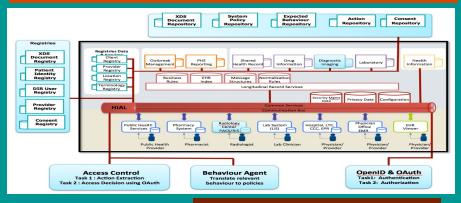
Simulation of an Infrastructure for Secure Sharing of Medical Images between PACS and EHR Systems

Kamran Sartipi
Krupa A. Kuriakose
Weina Ma
University of Ontario Institute of Technology
{Kamran.Sartipi, Krupa.Kuriakose, Weina.Ma}@uoit.ca

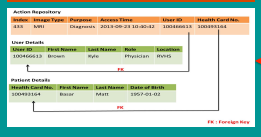
Approach for Secure medical Image Sharing

PACS (Picture Archiving and Communication Systems) are legacy systems that are used for storing and retrieving medical images. To restrict the privacy breaches or to prevent intrusion from outside, the functionality of the existing PACS are localized to their working environment. PACS do not provide any external interfaces that allow systems to interact with other PACS or with a common infrastructure for authentication, authorization and audit. We propose a new infrastructure for secure medical image sharing between legacy PACS and DI-r. The solution employs OpenID standard for user authentication, OAuth service to grant authorization and IHE XDS-I profiles to store and retrieve medical images and associated meta data. In the proposed infrastructure cooperative agents are employed to provide a user action and patient consent based access control mechanism to share medical images. This allows safe integration of PACS and DI-r systems within a standard EHR system. In addition to this, a behavior-pattern based security policy enhancement feature is added to the system to assist the system security administrator. The resulting secure and interoperable medical imaging systems are easy to expand and maintain. Behavior of the entire system is analysed using general-purpose model driven development tool IBM Rational Rhapsody. The code generation and animation capability of the tool makes it powerful for running effective simulations. We mainly explore the use of statecharts and their interactions with MySQL database to learn the behavior of the system.

Overall view of Canada Health Infoway's EHR Architecture augmented by the proposed infrastructure (blue components)



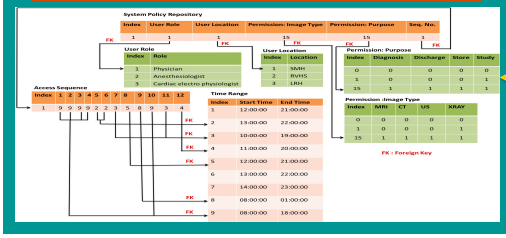
Schemas for database designed in MySQL DB for action repository



- When the user approaches the PACS system to retrieve an image from the DI-r, the "Access Control" component captures the relevant information of the user required for making access control decisions.
- We call this interaction an "Action" of the user. The attributes of these interactions are recorded according to an "Action Tuple" as follows:

Action Tuple = *<User, Role, User Location, Server Location, Time of Day, Requested Data Type, Purpose of access>*

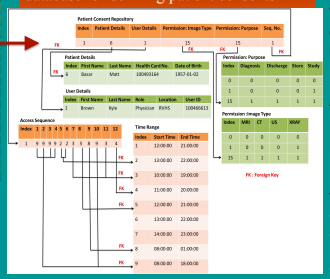
Schemas for database designed in MySQL DB for defining system policies



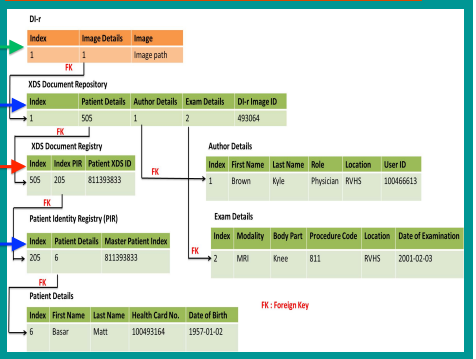
User Interface designed in IBM Rational Rhapsody

Statechart of Access Control, OpenID and XDS-I module to store and retrieve image

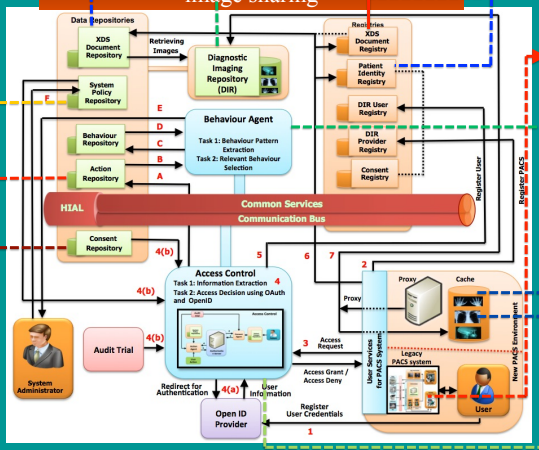
Schemas for database designed in MySQL database for defining patient consents



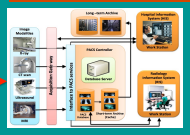
Schemas for database designed in MySQL database for XDS-I profile



Proposed secure framework for PACS image sharing



Legacy PACS system



Behavior pattern of user extracted by applying Apriori Algorithm

Length of Sequence	Frequency of Occurrence	Sequences
8	10	7 8 12 13 15 16 20 21
7	10	7 8 12 13 15 16 20, 7 8 12 13 15 20 21, 8 12 13 15 16 20 21
6	12	7 8 12 13 15 20
6	10	12 13 15 16 20 21 , 8 12 13 15 16 20 , 7 8 12 13 15 16
5	12	8 12 13 15 20 , 7 8 12 13 15 , 7 12 13 15 20
5	11	13 15 16 20 21, 7 8 15 16 20
5	10	7 8 12 16 21, 7 8 13 15 16 , 8 12 13 15 16, 8 13 16 20 21 , 12 13 15 16 20 , 13 15 16 20 21

Image retrieved from DI-r (receiver – PACS A)

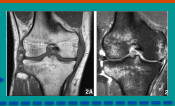
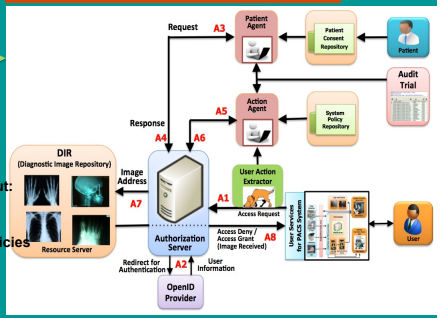


Image retrieved from DI-r (receiver – PACS B)

Access Control process using OAuth Authorisation Protocol



The core of the Access Control component is the "Authorization Server".

To make proper access control decisions, Authorization Server must receive the information about:
i) user's authentication
ii) nature of the access operation that complies with the system policies
iii) patient's consent directives
iv) Audit trails

The Authorization Server performs two main functions:

- Authorization grant and delivering the Access Token to the user service.
- Authorisation grant is given to the user service after authenticating the user and consulting with the "Patient Agent" and "Action Agent ".
- If both the Patient Agent and Action Agent approve the user's requested operation to the Authorization Server, the Authorization Server issues an "Access Token" to the user.
- User using the Access Token requests the protected patient's medical image and associated metadata from the DI-r and associated XDS repository respectively.