i2b2 Software Architecture

Project Management (PM) Cell

Document Version: *1.7.08-004*

i2b2 Software Version: *1.7.08*

TABLE OF CONTENTS

DOCUMENT MANAGEMENT

Revision Number	Date	Author	Description of change
1.7.1	11/06/12	Janice Donahoe	Created the 1.7 version of this document.
1.7.2	10/23/13	Mike Mendis	Updated JBoss and Axis2
1.7.00-003	08/12/2015	Janice Donahoe	Fixed Document Version information that appears on the cover page. This was never updated to 1.7.2. It has now been updated to 1.7.00-003. Also fixed some minor spelling issues.
1.7.08-004	04/27/2016	Janice Donahoe	Fixed title page and some minor formatting. Content did not change.

ABSTRACT

This is a software architecture document for the **Project Management (PM) cell**. It identifies and explains the important architectural elements. This document will serve the needs of stake holders to understand the system concepts and give a brief summary of the use of the PM message format.

1 OVERVIEW

The Project Management cell (PM) is an i2b2 Hive core cell and it has two basic functions:

1. To control user access to various services
2. To keep track of where these services are located

User access is determined by a user's "*role*", which is a variable associated with a user that serves to define the actions that a user may perform. The role may determine how much data to return and whether or not there is access to a particular service.

> **Note**
>
> Roles are further defined in the next section, which is called *User Roles*.

In addition to roles, there is the concept of a "*target location*" or "*domain*" that further defines the environment and associated permissions. The target location is a variable that defines the PM server location to be accessed. When a person logs in to the i2b2 Workbench, a login screen comes up that requires the username, password and target location to be entered. The target location is also called the domain, which is shorthand for domain name and it is used to authenticate the user. The domain is actually shorthand for the domain name. The i2b2 cells have mappings of the domain names to the URLs; these mappings tell where the service that will authenticate the user is located. If the domain does not exist in the lookup table, the person is not authenticated. If the domain exists, the user is authenticated. In effect, the mapping of the domain name to the URL provides an extra layer of security to the **authentication process**.

After the authentication process the PM cell performs the **authorization process**. The **get_user_configuration** message is used by the PM cell to determine the user's roles, permissions and privileges as well as return what the user is allowed to see.

1.1 User Roles

The PM determines when and how the data is presented to a user based on their project user roles. Each user will have at least two roles per user_id and product_id combination. These two roles can be further defined as a *Data Protection role* and a *Hive Management role*.

The data protection role / path establish the detail of data the user can see while the hive management role / path defines the level of functionality the user has in a project. The following tables summarize the roles in a hierarchical order of least to most access.

Data Protection Track	
Role	**Access Description**
DATA_OBFSC	OBFSC = Obfuscated ▪ The user can see aggregated results that are obfuscated (example: patient count). ▪ The user is limited on the number of times they can run the same query within a specified time period. If the user exceeds the maximum number of times then their account will be locked and only the Admin user can unlock it.
DATA_AGG	AGG = Aggregated ▪ The user can see aggregated results like the patient count. ▪ The results are not obfuscated and the user is not limited to the number of times they can run the same query.
DATA_LDS	LDS = Limited Data Set ▪ The user can see all fields except for those that are encrypted. ▪ An example of an encrypted field is the *blob fields* in the *fact* and *dimension tables*.
DATA_DEID	DEID = De-identified Data ▪ The user can see all fields including those that are encrypted. ▪ An example of an encrypted field is the *blob fields* in the *fact* and *dimension tables*.
DATA_PROT	PROT = Protected ▪ The user can see all data, including the identified data that resides in the Identity Management Cell.

Hive Management Track	
Role	**Access Description**
USER	Can create queries and access them if he / she is the owner of the query
MANAGER	Can create queries as well as access queries created by different users within the project

Note

Additional roles can be added to the PM_PROJECT_USER_ROLES table but there will not be any

recognized hierarchy to those roles.

1.2 Security: User Authentication

Users may access the PM with a user_id and password combination. Secure http (https) can be used to encrypt the username, password and all transmitted data to and from the PM cell.

1.3 Technical Platform

The technology used to build the product is as follows:

- Java 2 Standard Edition 7.0
- Oracle Server 10g/11g database
- SQL Server 2005/2008
- Xerces2 XML parser
- Jboss Application server version 7.1.1
- Spring Web Framework 2.0
- Axis2 1.6.2 web service (SOAP / REST)

1.3.1 Security

The application must implement basic security behaviors:

Category	Behavior
Authentication	Authenticate using at least a user name and a password.
Authorization	Based on the user role, the user may only access categories they have been given permission to access.
Confidentiality	Sensitive data must be encrypted (Patient Notes).
Data Integrity	Data sent across the network cannot be modified by a tier.

Auditing	In the later releases we may implement logging of sensitive actions.

1.3.2 Persistence

This application utilizes JDBC calls to retrieve persisted data.

1.3.3 Reliability / Availability

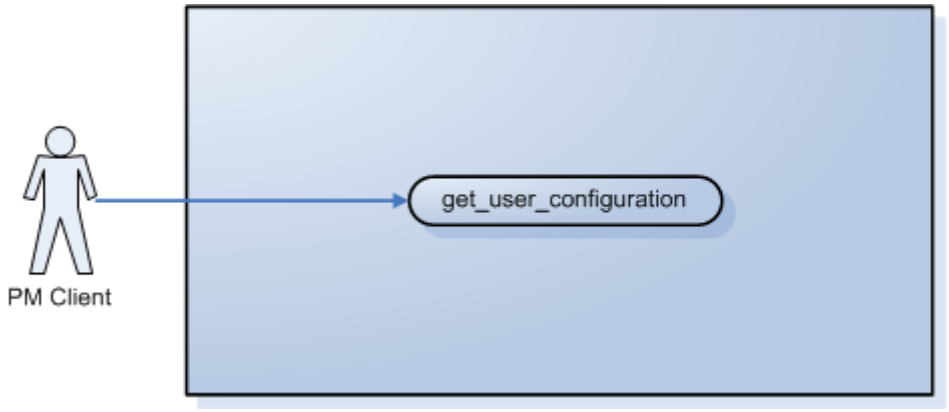
- The reliability / availability will be addressed through the J2EE platform
- Targeted availability is 16 / 7: 16 hours a day, 7 days a week
- The remaining time (8 hours) is reserved for any maintenance activities

1.3.4 Performance

- The user authentication with the project management cell must be under 10 seconds.

2 USE CASE

The diagram below depicts common use cases a user may perform with the PM cell.



Additional Resources

The *Project_Management_Messaging* document contains a complete list of detailed use cases.

2.1 Operations

The PM service is designed as a collection of operations or use cases:

Service	Description
get_user_configuration	Returns a list of project and roles available for a given user. Also all the services cell information for the hive is provided.

Additional Resources

The *Project_Management_Messaging* document contains a complete list of operations.

3 ARCHITECTURE DESCRIPTION

This section provides a description of the architecture as multiple views. Each view conveys the different attributes of the architecture.

1. Components and Connector View
    a. Client-Server Style

2. Module View
    a. Decomposition Style
    b. Uses Style

3. Data View
4. Deployment View

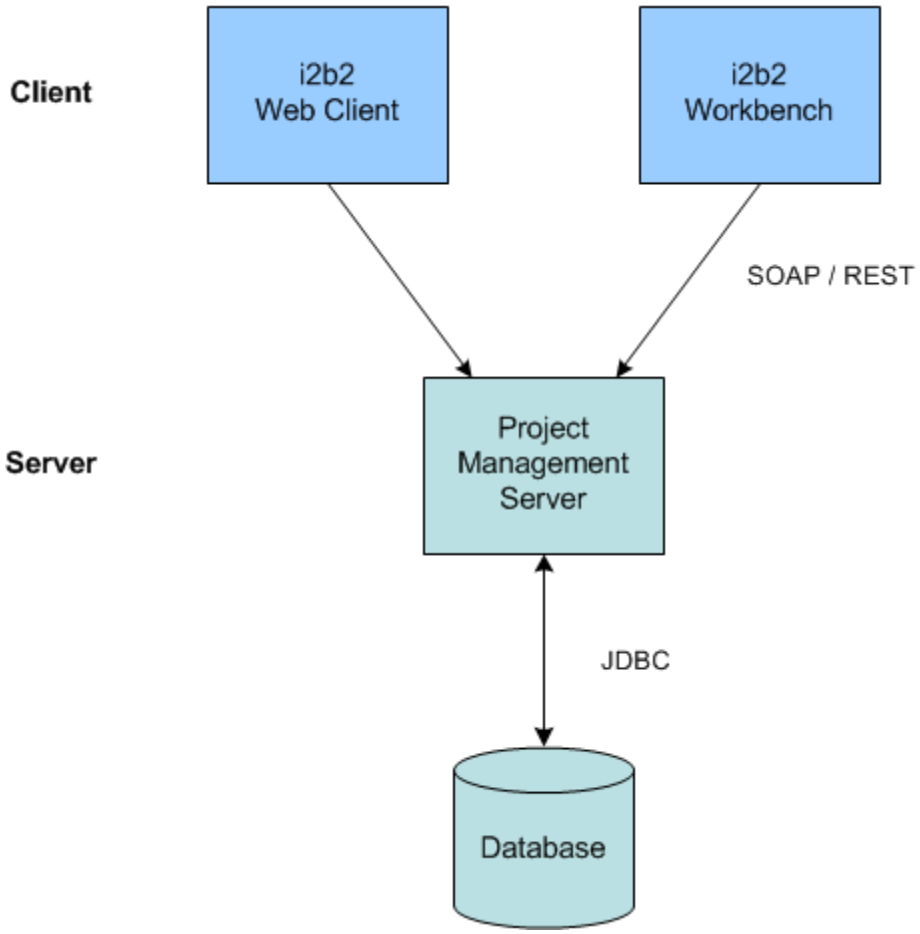
3.1 Components and Connector View

A **Component and Connector view** (C&C) represents the runtime instances and the protocols of connection between the instances. The connectors represent the properties such as concurrency, protocols and information flows. The diagram shown in the *Primary Presentation* section represents the Component and Connector view for the multi-user installation. As seen in the diagram, component instances are shown in more detail with specific connectors drawn in different notations.

3.1.1 Client-Server Style

The PM system is represented using the C&C Client-Server view.

3.1.1.1 Primary Presentation



3.1.1.2 Element Catalog

The properties of PM cell elements are:

- *Element Name:* listed in the table shown below.
- *Type:* whether the element is a data repository, a data accessor, a communication method, a query, a client or a server component.
- A *description* of the element

Element Name	Type	Description
i2b2 Workbench	Client Component	Webservice client submits the requests to the PM server components and renders a response XML.
Project Management Server	Server	The ONT cell uses the PM cell to authenticate the user.

	Component	The ONT cell constructs the PM request message and makes a web service call to the PM cell.
db	Data Repository Component	This repository is a database for the cell, group, role, and user information.
JDBC	Query Connector	SQL query used as a connector between the PM System and the metadata DB.
Web Service	Request Connector	SOAP or REST request used to communicate with the external system.

3.1.1.3 Design Rationale, Constraints

N-tier Architecture

The client-server style depicts the n-tier architecture that separates presentation layer from business logic and data access layer; thus providing for a high degree of portability.

3.2 Module View type

The module view shows how the system is decomposed into implementation units and how the functionality is allocated to these units.

- The layers show how modules are encapsulated and structured.
- The layers represent the “allowed-to-use” relation.

The sections that follow will describe the module view using Decomposition and Uses Style.

3.2.1 Decomposition Style

The Decomposition style presents the functionality in terms of manageable work pieces. They can be further decomposed to present higher level of details. The decomposition view identifies modules and breaks them down into sub-modules and so on, until a desired level of granularity is achieved.

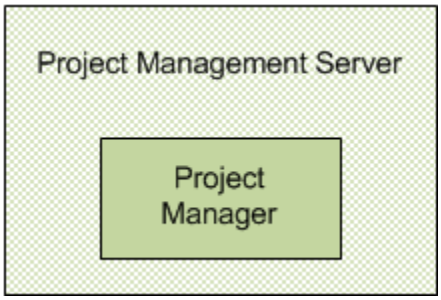
3.2.1.1 Primary Presentation

System	Segment
Project Management Server	Project Manager

3.2.1.2 Element Catalog

Element Name	Type	Description
Project Manager	Subsystem	This subsystem manages queries for the user and cell operations.

3.2.1.3 Context Diagram



3.2.2 Uses Style

The Uses style shows the relationship between modules and sub-modules. This view is very helpful for implementing, integrating and testing the system.

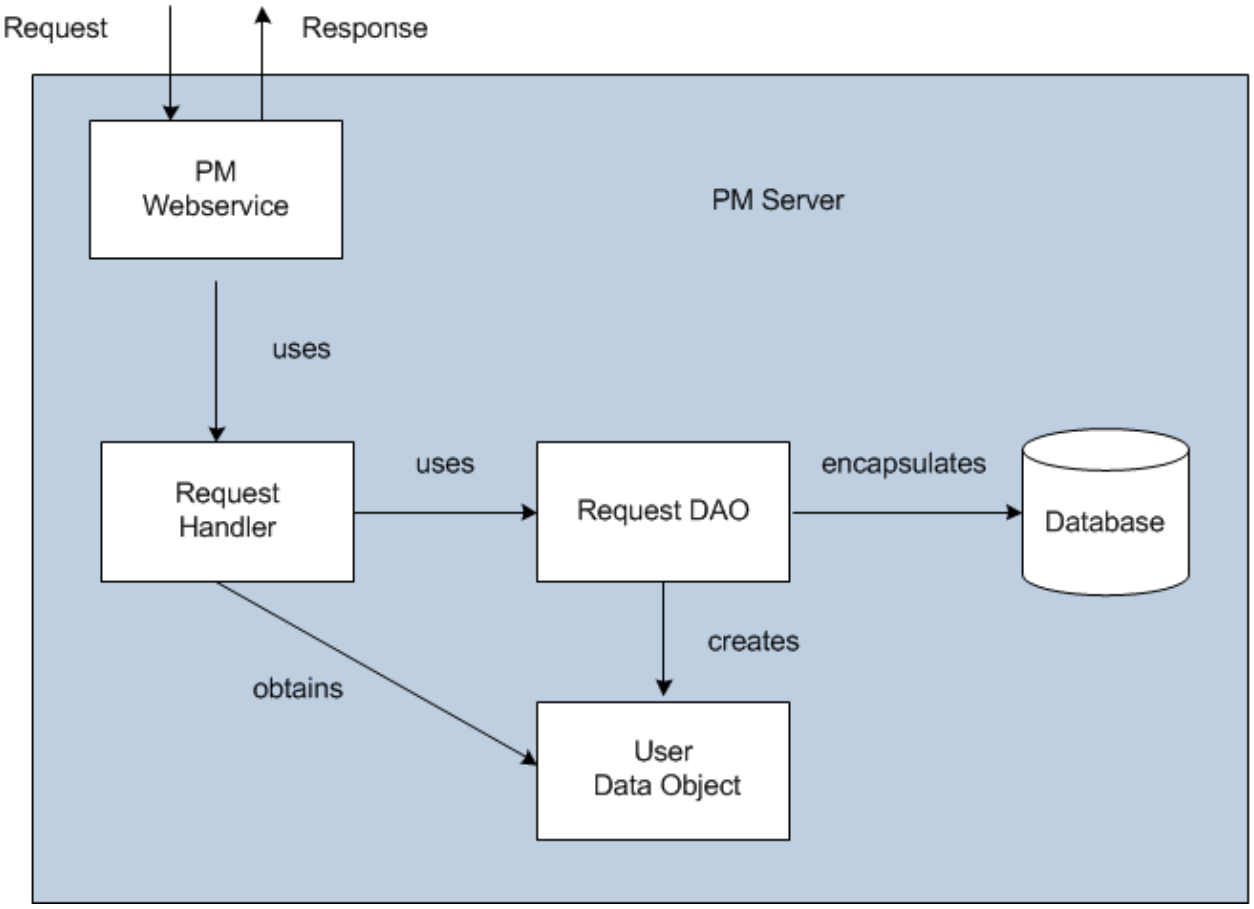
3.2.2.1 Primary Presentation

System	Segment
Project Management Server	PM Module
Project Manager Subsystem	PM Webservice
	Request Handler
	Request DAO
	User Data Object

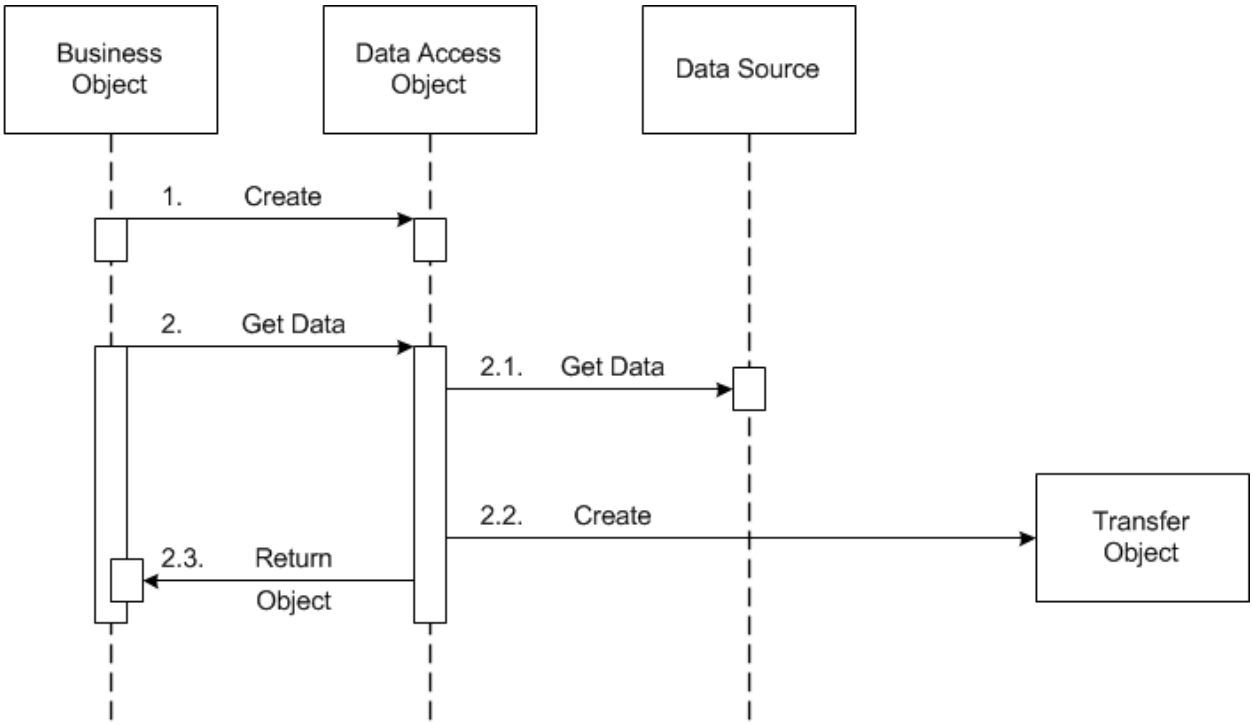
3.2.2.2 Element Catalog

Element Name	Type	Description
PM Module	Module	Authenticates the user through local user name or active directory.
PM Webservice	Communication Module	Provides web service interface to project manager operations.
Request Handler	Business Object	Delegates requests to the data access object (DAO) layer to perform database operations.
Request DAO	Data Access Object	Supports database query operations.
User Data Object	Transfer Object	Object representation of persisted data

3.2.2.3 Context Diagram



3.2.2.4 Sequence Diagram



3.3 Mappings of Styles

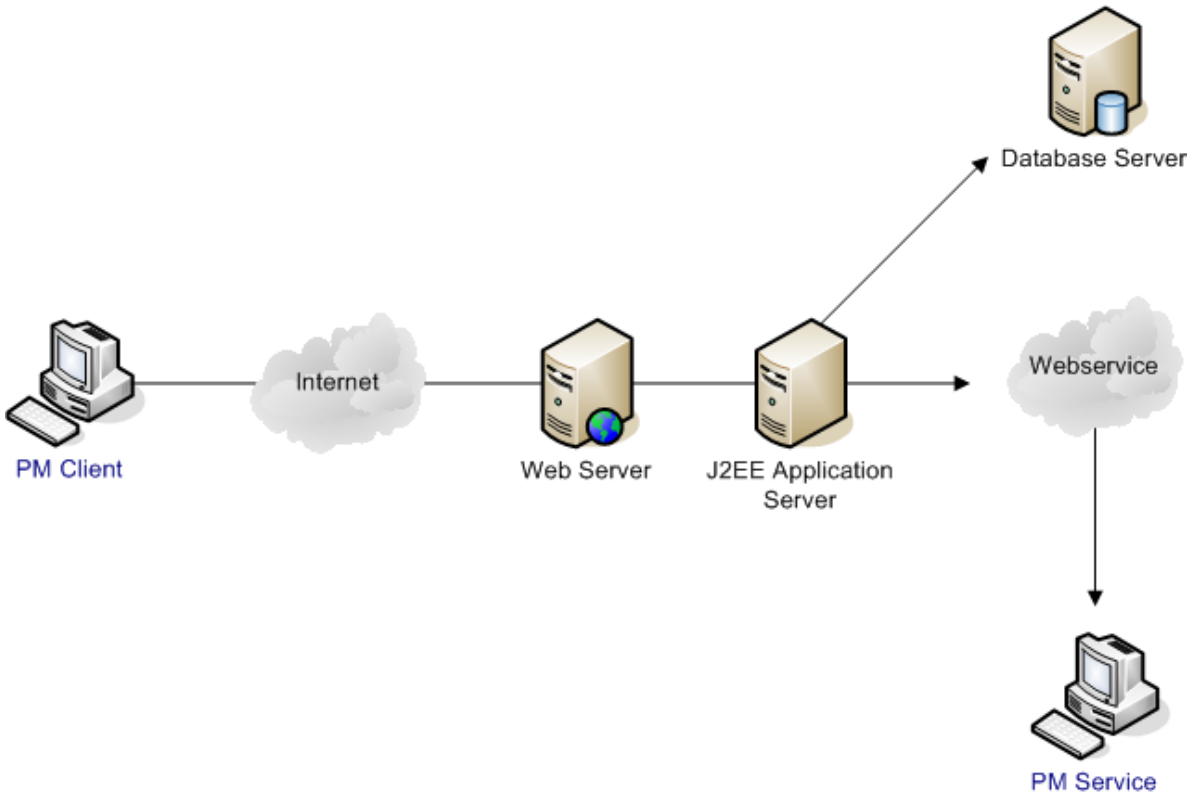
The following table is a mapping between the elements in the *Component & Connector Client-Server style* shown in section 3.1.1, and the *Modules Uses view* and *Decomposition style show* in sections 3.2.1 and 3.2.2.

The relationship shown is ***is-implemented-by***, i.e. the elements from the components and connector view shown at the top of the table are implemented by any selected elements from the Modules views, denoted by and “X” in the corresponding cell.

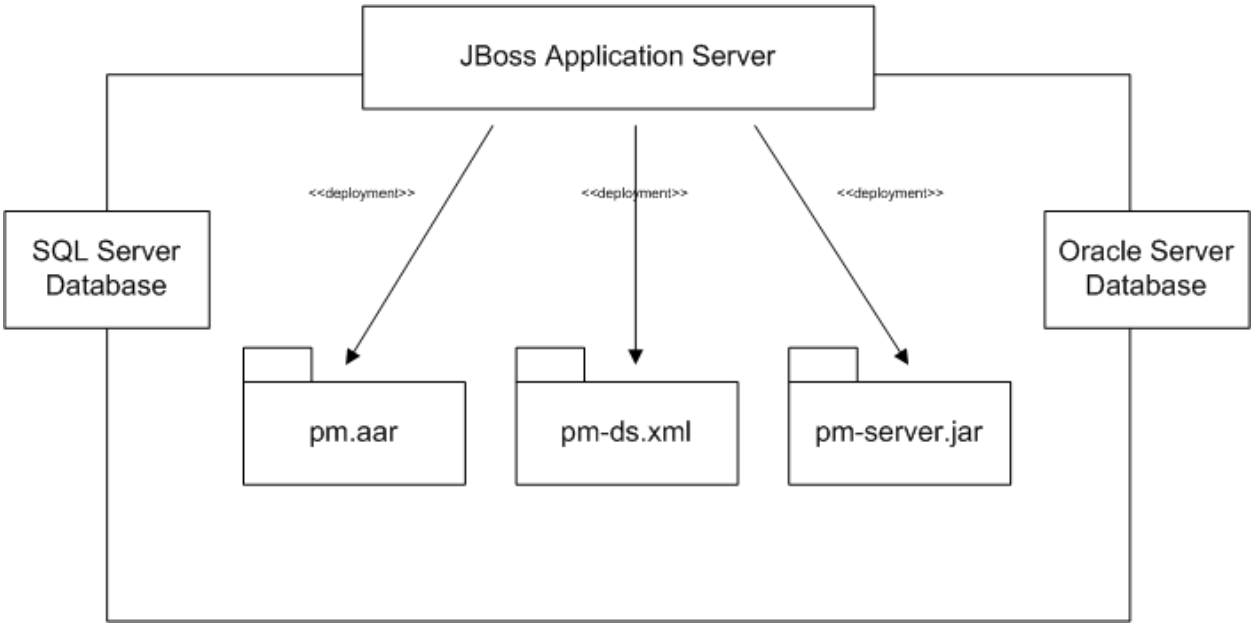
	PM Server	**Metadata Database**
PM Service	X	
PM Webservice	X	
Request Handler	X	
Request DAO	X	X
User Data Object	X	

4 DEPLOYMENT VIEW

4.1 Global Overview



4.2 Detailed Deployment Model



REFERENCES

i2b2 (Informatics for Integrating Biology and the Bedside) *https://www.i2b2.og/resrcs/hive.html*