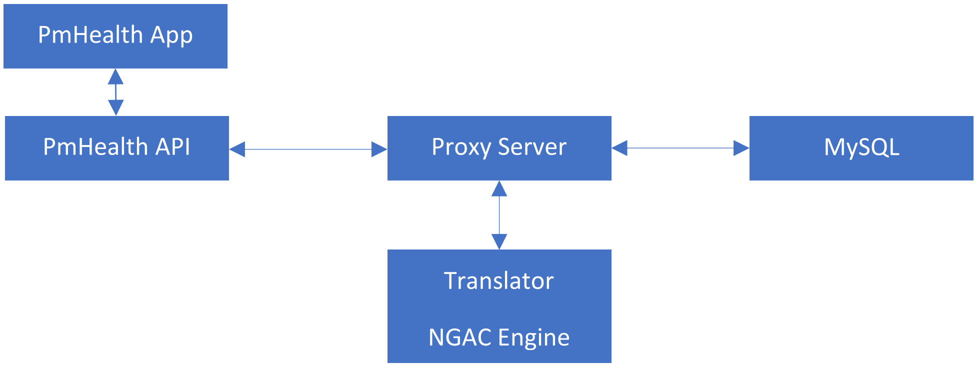
Next Generation Database Access Control (NDAC)

I. Setup



A. Prerequisites

- Tomcat
  1. Run the tomcat startup script in $CATALINA_HOME\bin\startup
  2. add the following text to $CATALINA_HOME\conf\tomcat-users

```
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<user username="admin" password="password" roles="manager-gui, manager-script"/>
```

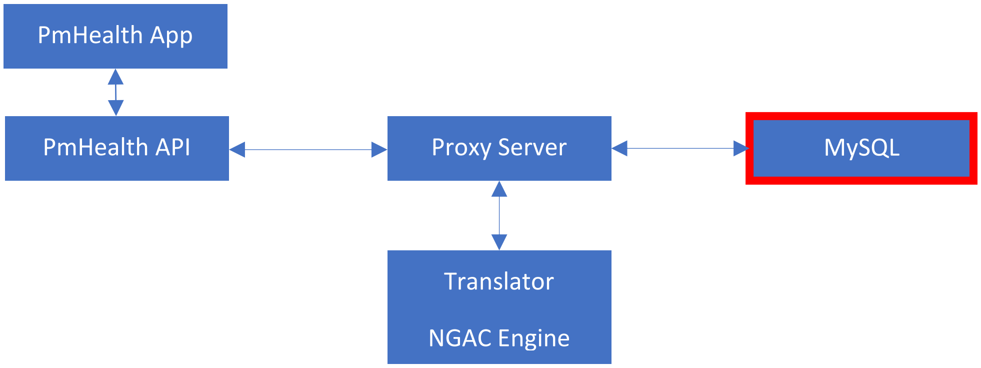
  3. Add a server to maven in ${MAVEN_HOME}/conf/settings.xml

```
<server>
   <id>TomcatServer</id>
   <username>admin</username>
   <password>password</password>
</server>
```

- Npm
- Angular
  1. npm install -g @angular/cli
- MySQL
- Neo4j (if using Neo4j for NGAC Engine)

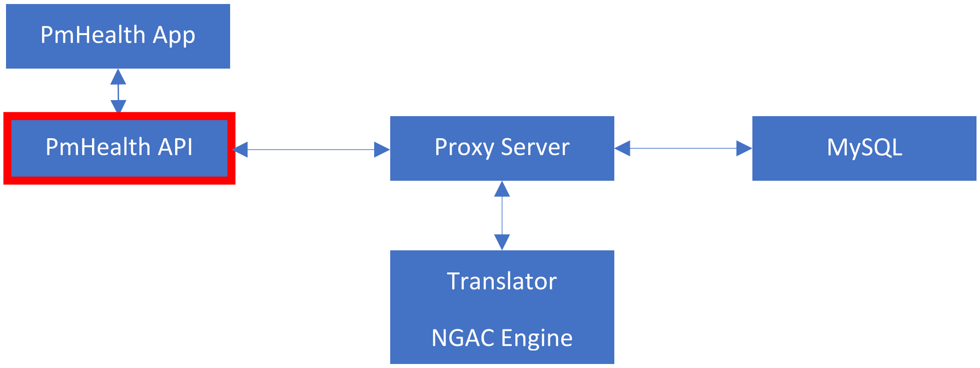
B. PmHealth Demo Application

- **MySQL Database**



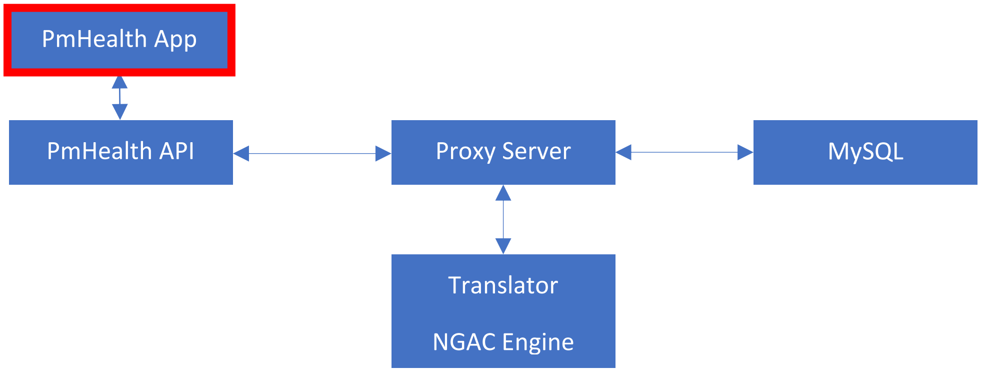
1. Run ndac_demo.sql in PmHealthApi/db/. This will create the pm_health schema.

- **JAX-RS/Tomcat Back End**



1. In the project’s root directory, run ‘mvn install’.
2. Run ‘mvn tomcat7:deploy’.
3. The application will be available at localhost:8080/pmhealth.

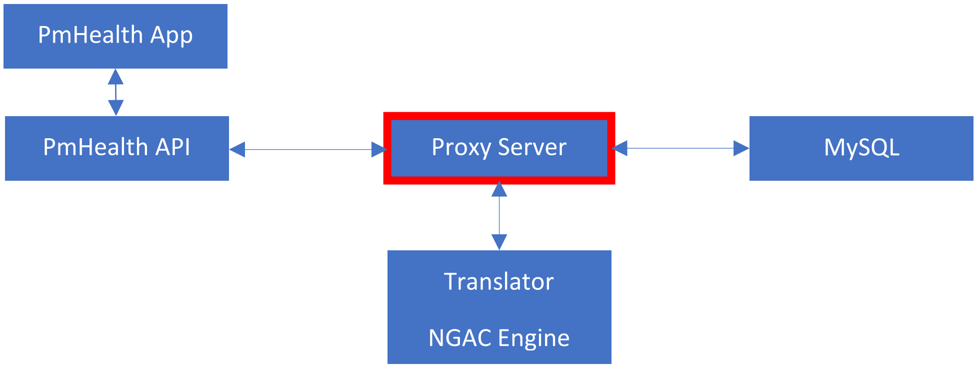
- **Angular Front End**



1. In the project’s root directory, run ‘npm install’.
2. Run ng serve –o, and the application will open at localhost:4200.

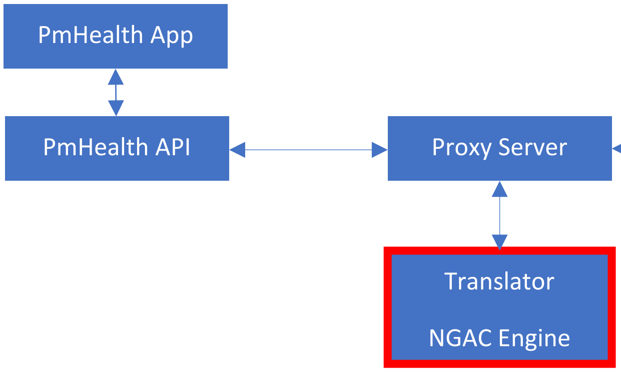
C. NDAC Elements

- **Proxy Server**



1. In the root directory of PmProxy, run ‘java -jar PmProxy.jar’ to start the proxy server, which listens on port 5050.

- **NGAC Engine and Translator**



1. In the project's root directory, run 'mvn install'.
2. Run 'mvn tomcat7:deploy'.
3. The application will be available at localhost:8080/pm.
4. Go to localhost:8080/pm/config.jsp.
5. Select Neo4j or MySQL and connect.
6. In the 'Load Configuration Script' section, click 'browse' and locate the file 'ndac_demo.pm' in PM/config.
7. Click 'Load Configuration' to load the demo configuration into the database

II. **Access Control Policies** (Read permissions only)

There are 3 Policy Classes Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Experimental Drug Policy (EDP) and 6 Users Bob, Alice, Chris, Betty, Emily, and Lucy. In the RBAC Policies there are 4 roles: Doctor, Patient, Nurse, Clerk. Bob and Alice are doctors, Chris and Betty are patients, Emily is a nurse, and Lucy is a clerk. Each doctor has access to one patient's record. Bob has access to Chris' and Alice has access to Betty's. Nurses have access to visit information such as admission and discharge dates, the reason for the visit, and vitals taken during the visit. Under RBAC, they also have access to the other fields such as treatments, diagnoses, etc.

In DAC, each user has a home container which they have access to. In this configuration, Chris' Record is in his home container as well as Bob's. Similarly, Betty's record is in her own home container and that of Alice. Lucy (clerk) has just the patient info and basic visit information of both records in her home container. Emily (nurse) has the non-sensitive patient information, basic visit information, and vitals for both records in her home container. In this configuration, she has also been granted access to Betty's record as if Alice we're delegating responsibilities to her. This means that Emily has access to Betty's complete record, while still only having the basic information on Chris' record.

EDP has two attributes: edp_patients and edp_doctors. Alice has the edp_doctors attribute, Betty has the edp_patients attribute. There are prescriptions in Betty's record called 'Top Secret Cancer Drug'. The edp_patients attribute allows Betty to see the prescriptions for her record and the edp_doctors attribute allows Alice to see anything assigned to this container. Emily, however, does not have access to the objects in this policy. Therefore she will be unable to access them but will be able to access any other data that is not in this policy.

III. **Demo Script**

1. Notes:
   a. Each user's password is the same as their username (i.e username=bob, password=bob)

   b. The current state of the NDAC demo only demonstrates read permissions using select statements

2. As Bob, click on the ‘Patients’ link. Click on Chris Smith’s record.
3. Bob will be able to read the whole record
4. As Chris, click on the ‘My Record’ link to view his own record. He will be able to read everything except the doctor note field for his visits as these are only accessible by doctors.
5. As Alice, click the ‘Patients’ link and open Betty’s record. She will be able to view all of it. Including prescriptions called ‘Top Secret Cancer Drug’. This data has been protected under the Experimental Drug Policy and only Alice and Betty can read it.
6. As Betty, Open her own record and confirm she can read the entire record including the prescriptions mentioned above.
7. As Emily, click the ‘Patients’ link and open Chris’ record. She can see basic visit information and the vitals for each visit
8. Still as Emily, open Betty’s record. Emily has been granted access to her entire record and can therefore see all fields. However, since Emily does not have permission for the ‘Top Secret Cancer Drug’ under EDP, she is unable to see that information.