**Implementation – 11/1/2016**

**Steps (as shown in figure):**

1. Input YANG file from end user with high level information like host names or website names.
2. Security Controller
3. processes the input YANG file
4. searches for the host names from the list of host names stored in the controller
5. if host name is found in its file, it replaces the host name with it’s corresponding ip address
6. Security Controller initiates a socket communication to NSF to transfer the translated YANG file.
7. NSF accepts the socket communication from the controller and receives the translated YANG file.

1. Input YANG file: “file.yang”

2. Translate Input file

Security Controller

4. Implement the YANG file

NSF

3. Translated Input YANG file: “file.yang”

**Implementation language:** JAVA

**Execution Process:**

1. Execute the program in the controller VM
2. Once controller is started, execute the program in NSF

VM Controller IP: 10.155.14.180

VM NSF IP: 10.155.14.181

**Work In-Progress:**

Step 4: NSF should be able to successfully implement the YANG input file from the Controller

Step 2: Use ConfD to handle multiple NSFs and to enforce YANG data models on the NSFs

Step 1 and Step 3: Use secure connection channel (TLS) or any encryption to encrypt the input and translated YANG files.

Step 2: Support for providing better Natural language processing (For eg: with inappropriate host names)

**Challenges:**

* Processing the input file with YANG supported syntax
* Achieving accuracy in detecting required information (host names, website names) and replacing it with accurate and appropriate information (IP addresses)
* Configuring NSF to accept information from Controller