**ML Model Deployments**

*Introduction:*

Model deployment is the last stage of ML/AI project and engineers/researchers must ensure the implemented model is available for end-users to use the same.

Further, many parameters to be considered before deploying the model, such as,

(i) data storage

(ii) end user/client/stakeholder

(iii) number of users

(iv) monitoring strategy and few more.

In this section, major deployment models have been explained in detail. In all our samples, IRIS model sample has been used. As the first part of learning the deployment approaches, we need to learn the workflow of machine learning model.

*Machine Learning Model Workflow*

In the normal development lifecycle of machine learning model, model will be implemented first and it will be made available to the use to test the performance or end-users' access. The simple model's workflow has been shown in the diagram [1]. Upon deploying the machine learning model, user will send the prediction request via any user interface. User interface will accept user's input and send or forward the same to web server, and webserver will delegate the prediction request to machine learning model, get the response back and send the response to the user interface. Finally, user will be given the prediction result for the submitted query.

*[Diagram 1] Visual Representation of Machine Learning Model Workflow*

Machine generated alternative text:
User access UI to send 
prediction requests 
and receive 
responses. 
User 
Interface 
Machine 
Learning Model 
to 
espoose f 
ro 
Serv 
Web Framework 
(Flask/etc) 

The workflow shown in the diagram[1] can be customized further based on the complexity of the model and environment setup.

*Save and Load the model file:*

We should be able to finalize the implemented model only after testing the model with new data and comparing the model with other models. In this section, we have taken a simple IRIS model for experimenting all the deployment types. As the main target is about learn the different deployment types, less priority has been given to train and validate the model. Once the basic model is trained, it will must be saved and restored/reloaded for the later of deployment. There are two approaches , namely (i) Pickle and (ii) Joblib has been selected to test the save/load logic.

TODO : Install Pickle and Joblib

(i) Pickle Method

Pickle is a python library, has been used for serialization/de-serialization. i.e. it has been used to store the structured data into file and restore the same from the desk. It offers dump() method to save and load() method to load the content from the disk.

| #pickle file name to store and load the model  pickle\_filename = "Iris\_Classifer.pkl"    #save the model  with open(pickle\_filename, "wb") as file:  pickle.dump(model, file)    #load the model  with open(pickle\_filename, 'rb') as file:  iris\_model\_pickle = pickle.load(file) |
| --- |

Above few lines of code shows that how to save and load the pickle file. First, filename string is initialized and next section saves the model (has the trained model) into the given filename (i.e. pickle\_filename = "Iris\_Classifer.pkl"). The file mode "wb" refers that write mode in binary format. Subsequently, same file has been opened in "rb" mode (read mode for binary file) and loaded from the disk for the further usage.

(ii) Joblib Method

The Joblib Module comes part of Scikit Learn package and it can be used as the replacement for Pickle. One of the advantages of using this module is, it doesn't require the additional file object to save/load the model. Further, Joblib library is more efficient when it deals with large array and below few lines of code shows show how the joblib can be used to save and restore the model.

| #joblib file name to store and load the model  joblib\_filename = "Iris\_Classifer.jbl"  joblib.dump(model, joblib\_filename)    #load the model  iris\_model\_joblib = joblib.load(joblib\_filename) |
| --- |

First, filename is initialized and model object is saved in disk using the method dump. Afterwards, load() method is called to restore the saved file. As Jobllib is more efficient and easy to use, Joblib library has been used in all the deployment samples for loading the file.

Full Code (filename : iris\_model.py)

TODO: copy Full code

*Explanation:*

The programs starts with importing all the required libraries. Upon importing the required libraries, iris dataset has been loaded from the github repository and saved in a variable "dataset". The first four columns' values and last 'Y' column values are extracted and saved in separate variables, 'X' and 'Y' respectively . The "train\_test\_split" API has been used to split the given dataset into 70% training and 30% test datasets. The SVM(Support Vector Machine) library's SVC(Support Vector Classification) implementation has been used as classification algorithm. The SVC method uses RBF(Radial Basis Function) Kernel as default and gamma value(SVM performance parameter) is set to auto. In the following lines, model is trained using "fit" method and validation results have been obtained by calling "predict" function from the model with "x\_validations" parameter.

Though we don’t focus more on the model accuracy here, the following lines prints the accuracy score, confusion matrix and classification report evaluation metrics. Lastly, trained model has been saved and restored using Pickle as well as Joblib approaches.

*Run the source code:*

> python iris\_model.py

Output :

| Accuracy Score : 97.77777777777777  Confusion Matrix :  [[11 0 0]  [ 0 17 1]  [ 0 0 16]]  Classification Report :  precision recall f1-score support    Iris-setosa 1.00 1.00 1.00 11  Iris-versicolor 1.00 0.94 0.97 18  Iris-virginica 0.94 1.00 0.97 16    accuracy 0.98 45  macro avg 0.98 0.98 0.98 45  weighted avg 0.98 0.98 0.98 45    Prediction result(Pickle model file) for [5.1, 3.5, 1.4, 0.2] : Iris-setosa  Prediction result(Joblib model file) for [5.1, 3.5, 1.4, 0.2] : Iris-setosa |
| --- |

The result shows that trained model's evaluation metrics proves that model has been trained well. Finally, Pickle and Joblib can store and restore the model, and restored model is able to predict the result as expected. The code saves two files, namely, "Iris\_Classifer.pkl" (Pickle) and "Iris\_Classifer.jbl" (Joblib) in the current folder and the joblib file will be used in the rest of the deployment experiments.

1. **Using Flask Approach**

Flask is a web framework, written in python and it lets the developers to implement the web applications very easily. Its framework is categorized as microframework and it's based on WSGI(Web Server Gateway Interface) framework. The reason for categorizing Flask as microframework is, it's designed to have the core of the web application and easy to scale based on the requirement.

*Steps involved in ML model deployment*

(i) Build the model and save the same using Joblib.

(ii) Install Flask

(iii) Implement server side python app and expose API using flask.

(iv) Run the server

(v) Access the API using user interface.

As the very first step has been already completed, the steps from (ii) to (v) been explained below:

*Command to install Flask*

pip install flask

The next important stage is to implement the python application to use Flask and expose API. The simple Flask application code looks below:

from flask import Flask

app = Flask(\_\_name\_\_)

@app.route('/')

def home():

return 'Flask is active...!'

The very first line import the Flask class and an instance of this class will act as WSGI application. In the following line, Flask class's instance has been created and the argument \_\_name\_\_ has been passed. We may pass different argument if required but this argument is essential to Flask to know the place to look for the templates and other resources. The route() decorator carries the URL detail and this has been mapped to the triggering function. When the user calls the URL from the UI, linked function will be executed to process and give response to the user request.

Finally, Flask's instance run() function to be called to activate the server and the "debug=True" parameter has been passed to run the application in debug mode and the server application will be restarted if there is any changes made while running and helps to track the errors if any:

app.run(debug=True)

Full code (filename : model-depoyment-flask.py)

TODO: copy Full code

The Flask based deployment model code starts with importing the required modules, such as, Flask, request, json and joblib. In the following section, Flask's instance has been created and assigned to a global variable "app". As we have already saved the prediction model in the file "Iris\_Classifer.jbl", it has been restored/loaded using joblib and kept it in "joblib\_model" variable.

There are two APIs have been exposed, one is home and other one is predict-class. The home API URL is enabled to test the server is active or not. However, other API predict-class does the real prediction job. It takes four essential parameters(sepal-length, sepal-width, petal-length and petal-width) that require for the model prediction. Inside the "predict\_class" method, all the four parameters' values have been read and assigned to the different variables. The "predict" function of the model has been called with the four parameters and the result has been converted as json and returned to the caller.

Switch to the command prompt and locate the "model-depoyment-flask.py" folder and run the below command:

>python model-depoyment-flask.py

\* Serving Flask app "model-depoyment-flask" (lazy loading)

\* Environment: production

WARNING: This is a development server. Do not use it in a production deployment.

Use a production WSGI server instead.

\* Debug mode: on

\* Restarting with windowsapi reloader

\* Debugger is active!

\* Debugger PIN: 349-372-776

\* Running on <http://127.0.0.1:5000/> (Press CTRL+C to quit)

As shown above, Flask application is running on the local host (its default IP address 127.0.0.1) and listening to the port 5000. As the two APIs have been exposed in the flask server, copy the following urls, paste it on a web browser and press enter to see the result:

(a) <http://127.0.0.1:5000/>

Machine generated alternative text:
e 127.0.0.1:5000 
C 0 1270015000 
IRIS Classification Model(Flask based) is running successfully!!! 

(b) <http://127.0.0.1:5000/predict-class?sepal-length=5.1&sepal-width=3.5&petal-length=1.4&petal-width=0.2>

Machine generated alternative text:
127.0.0.1 x + 
C 0 127.0.0.1 1.4&petal-width=0.2 
{"predicted-result": "Iris-setosa"} 

As of now, we have tested our first Flask APIs using web browsers and this must the called from standard UI.

**2. Streamlit based Solution**

As of now, we have created our very first and simple ML deployment without any standard UI.

However, User Interface is very essential to easily access, enter/type the input and test the model. As the standard UI designing using technologies like Angular and React JS require significant effort, and it may not require for quick deployment, Streamlit based UI design and deployment for ML model has been explained in this chapter.

Streamlit is a simple and popular open-source framework, can be used to design very fast python based User Interface for ML projects. If the model owner does not have deep knowledge on UI development, Streamlit will be an incredibly good option as the Streamlit users do not need any prior knowledge on UI design to build a simple UI using python based Streamlit.

*Installing Streamlit library:*

pip install streamlit

The following simple Streamlit methods have been used in the deployment sample:

import streamlit as st

st.title("title text")

string\_value = st.text\_input('label text',0.0)

st.button("button label")

st.success('success message')

The streamlit library has been given an alias "st". The title() method is used to set the application title, text\_input() method receives single input from the user and return it as string. The major parameters of text\_input() methods are label text and default value. The button() method has been used to draw the button control with the given label. When the button is clicked, its code block will be executed. Finally, success() method used to show the success message on the UI and the message to be displayed has to be passed as the parameter of success() method.

TODO: copy Full code

Upon importing the required libraries, model filename has been initialized and load the file from the disk for the prediction. The python user defined method "preduct\_class" with four parameters has been added. This function call the predict function with given four parameters and return the predicted result the caller of the method. The second user defined method show\_UI() has very simple Streamlit code to show the UI components. The Streamlit user shows the title and four input controls to collect user’s input. Further, one button control (label : Predict Class) has been added. When the user clicks this button, its code block calls predict class() method for the prediction result. Finally, success() method is called with the predicted result to show it on the UI.

Run the Streamlit application:

Switch to the command prompt and locate the "model-deployment-streamlit.py" folder and run the below command:

>streamlit run model-deployment-streamlit.py

*You can now view your Streamlit app in your browser.*

*Local URL:* [*http://localhost:8501*](http://localhost:8501)

*Network URL:* [*http://192.168.0.103:8501*](http://192.168.0.103:8501)

The "Streamlit run" command has been used to run the Streamlit application from command line and it uses the port 8501 by default. We can copy any one of the url, paste it on the web browser and press enter. It will trigger the Streamlit that listen to the port 8501 and it displays the designed UI. Now, user can enter the four values in the input controls and click "Predict Class" button. It shows the predicted result just below the button.

Machine generated alternative text:
model-deployment-stream lit • St X 
C O localhost:8501 
IRIS Flower Classification 
septal-length 
0.0 
septal-width 
0.0 
petal-length 
0.0 
petal-width 
0.0 
Predict Class 
model-deployment-stream lit • St X 
C O localhost:8501 
IRIS Flower Classification 
septal-length 
5.1 
septal-width 
3.4 
petal-length 
1.1 
petal-width 
0.4 
Predict Class 
{"predicted-result": "Iris-setosa"} 

The UI on the left side shows the empty input controls and right side UI shows the filled input control with predicted result value.

**3. FastAPI**

The FastAPI is a python-based web framework, helps to create REST APIs very fast. It can be used as an alternative of Flask due to the following reasons:

(i) It's performance is high comparing with Flask.

(ii) Very stable web framework with fewer bugs.

(iii) Easy to learn and implement. Also, amazingly simple syntaxes help to reduce the code size.

(iv) It provides free swagger documentation. It helps the users to get the REST APIs list and parameters with zero dev effort.

Installing FastAPI :

*pip install fastapi*

Upon installing FastAPI, uvicorn also need to be installed to run the FastAPI. The following command can be used to install the uvicorn package:

*pip install uvicorn*

Minimum python code for FastAPI

from fastapi import FastAPI

#declare FastAPI instance

fastAPIInstance = FastAPI()

@fastAPIInstance.get('/')

def home():

return 'Fast API Home....'

The FastAPI gets enabled in python application by importing the FastAPI class from fastapi package. The following line, creates the instance of FastAPI and assign the class instance to the variable. Once the instance is created ( "fastAPIInstance "), routing methods need to be linked to the code for the response. In the above code, "get('/') refers the FastAPI home has been linked to the home() method. So when the user access the home URL from the browser, the linked method home() will be executed and it returns the response. So user can add different URIs and map different methods depends on the requirements.

TODO: copy Full code

The simple FastAPI based python code exposes two APIs outside, namely, (i) default or home and (ii) predict-class.

The first four lines, import the required packages for the application. In addition to the known packages, uvicorn has been added additionally.

Uvicorn is a lightning-fast ASGI(Asynchronous Server Gateway Interface) server implementation, ASGI is a successor of WSGI and it provide the interface between asynchronous behaviour python web servers, frameworks and applications. The WSGI provides synchronous behaviour and ASGI provides one for both asynchronous and synchronous apps.

Upon importing the packages, FastAPI() call is made to create an instance of FastAPI and it has been saved in the local variable "fastAPIInstance".

The subsequent lines, load the saved classification model from the disk for the prediction purpose. The first default REST API returns the text "ClassificationModel(FastAPIbased)isrunningsuccessfully!!!" when the url is home or default url is accessed. The second API has the main implementation to accept the users four input parameters, send the same to the trained/loaded model and receives the response back. Finally, received response has been converted to JSON and returns to the caller.

Running the FastAPI server code:

Switch to the command prompt and locate the "model-deployment-fast-api.py" file's folder and run the below command:

>uvicorn model-deployment-fast-api:fastAPIInstance --reload

[32mINFO[0m: Uvicorn running on [1mhttp://127.0.0.1:8000[0m (Press CTRL+C to quit)

[32mINFO[0m: Started reloader process [[36m[1m20544[0m] using [36m[1mstatreload[0m

[32mINFO[0m: Started server process [[36m16376[0m]

[32mINFO[0m: Waiting for application startup.

[32mINFO[0m: Application startup complete.

FastAPI runs on port number 8000 by default and the following table gives the clarity on the command and parameters being used to run the application.

| **uvicorn** | **ASGI server.** |
| --- | --- |
| model-deployment-fast-api | python file name which has the FastAPI server code. |
| fastAPIInstance | FastAPI class object. |
| --reload | flag that helps to reload automatically if there is any code changes. |

As we are already familiar with the endpoints and parameters, the two urls can be accessed as follows:

(i) Access the default/home URL : <http://127.0.0.1:8000/>

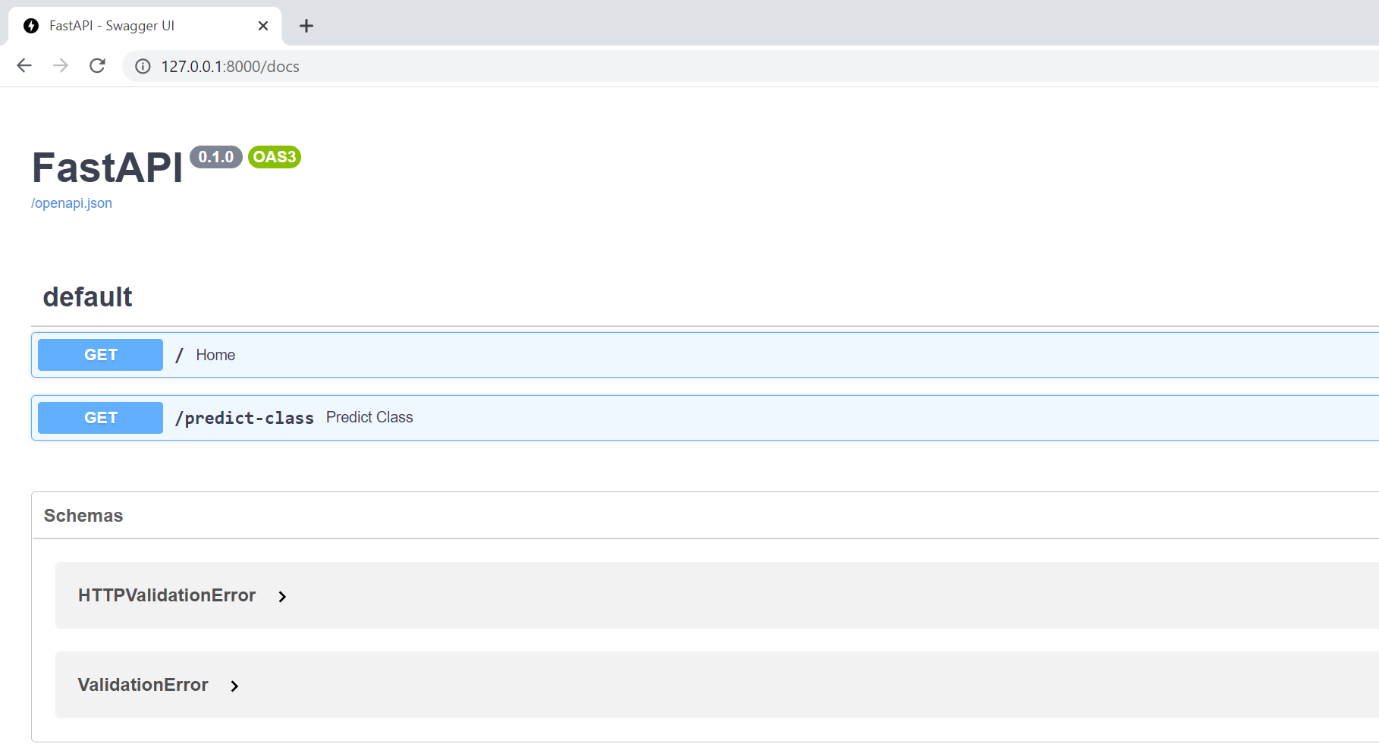
Machine generated alternative text:
e 127.0.0.1:8000 
C 0 127.0.0.1:8000 
"Classification Model(FastAPI based) is running successfully! ! ! " 

(ii) Access the predict-class for the given parameters: <http://127.0.0.1:8000/predict-class?sepal_length=5.1&sepal_width=3.5&petal_length=1.4&petal_width=0.2>

Machine generated alternative text:
127.0.0.1 x + 
C 0 127.0.0.1 width=3.5&petal length=l .4&petal width=0.2 
" { \ "predicted-result\ 
\ "Iris-setosa\ "Y' 

(iii) Accessing swagger documentations on the end points

The url "<http://127.0.0.1:8000/docs>" gives the list of exposed APIs and its parameters list for the easy access.



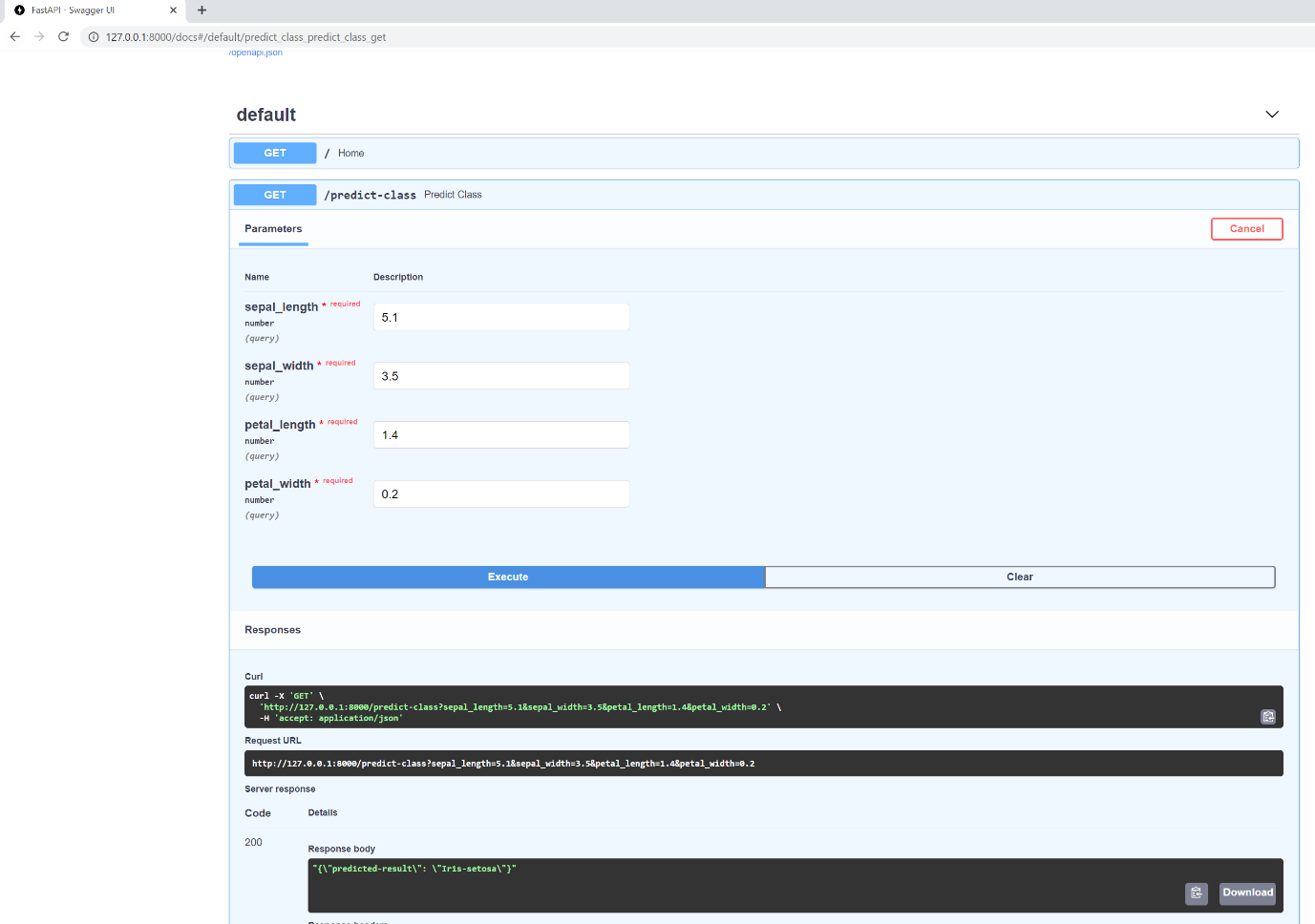
The APIs can be tested easily using the following steps:

(a) expand the predict class API detail by just clikicking on "Predict Class"

(b) click on the "Try out" button on the right top.

(c ) enter input values for the four parameters

(d) click on execute to see the below result:



(iv) Fancy documentation can be accessed using : <http://127.0.0.1:8000/redoc>

Machine generated alternative text:
x 
O 
FastAPl - ReDoc 
q Search... 
Home 
127.0.0.1 :8000/redoc 
FastAPI (0.1.0) 
Predict Class 
Download OpenAPl specification: 
Documentation Powered by ReDoc 
Home 
Responses 
> 200 Successful Response 
predict Class 
Download 
Response samples 
200 
Content type 
application/json 
null 
Copy 
/ predict—class 
QUERY PARAMETERS 
_H sepal length 
required 
sepal width 
required 
petal length 
required 
petal width 
required 
Response samples 
200 
422 
number (Sepal Length)l 
number (Sepal Width) 
number (Petal Length) 
number (Petal Width) 
Content type 
application/json 
Copy 
null 
Expand all 
Expand all 
Collapse all 
Collapse all 

4. Message Queue

Message queue mechanism gives the asynchronous solution to send request and receive response. In message queue, application send messages to receiver asynchronously and sender doesn't need to wait for the processed response immediately. A message will be sent to a queue and it will stay in queue until the receiver consume it.

A message can be any type of information and usually it will have task detail to be processed. The diagram [D12] shows the simple message queue. The enqueue typically insert/send the message inside the queue and all the messages inside the queue will be saved and served in FIFO manner. The Dequeue function remove the oldest message from the queue.

Machine generated alternative text:
MESSAGE 
Enqueue 
MESSAGE QUEUE 
MESSAGE #2 
MESSAGE 
Dequeue 

D12: Simple Message Queue (diagram from : <https://www.cloudamqp.com/blog/part1-rabbitmq-for-beginners-what-is-rabbitmq.html>)

Message queue can be used as inter-process communication medium, where the queue live inside the server. The consumers or workers will connect the queue and consume the message to process the task.

RabbitMQ

Machine generated alternative text:
Publish 
PRODUCER 
BROKER 
RabbitMQ 
Consume 
Subscribe 
CONSUMER 

D13 : RabbitMQ (diagram from : <https://www.cloudamqp.com/blog/part1-rabbitmq-for-beginners-what-is-rabbitmq.html>)

Proposed Customised flow

Machine generated alternative text:
Users 
Workers 
Message Queue 
Server 