BHUWAN CHANDRA

500067101

BATCH BAO B1

R103218033

**Assignment 2**

Q1. Types of cloud deployment models.

Different Types Of Cloud Computing Deployment Models

Most cloud hubs have tens of thousands of servers and storage devices to enable fast loading. It is often possible to choose a geographic area to put the data “closer” to users. Thus, deployment models for cloud computing are categorized based on their location. To know which model would best fit the requirements of your organization, let us first learn about the various types.

PUBLIC CLOUD

PRIAVTE CLOUD

COMMUNITY CLOUD

HYBRID CLOUD

MULTI CLOUD

Q2. Discuss Watson natural language classifier & Watson Retrieve and Rank.

You can use the Natural Language Classifier service with any objects in OpenPages but it is typically used to classify loss events, waivers, issues, and incidents. For example, you can use it to support your decision making when you classify a loss event to the correct Basel II categorization. You can also use it to support decision making when you classify waivers as exceptions to regulatory compliance. The text description that you enter is used as input to a Natural Language Classifier service that has been trained with knowledge from your domain specialists.

Terms to understand

**Natural Language Classifier**

A Watson service in IBM Cloud that uses machine learning algorithms to return the top-matching predefined classes for short text inputs. Your administrator configures, trains, and connects to a Natural Language Classifier service from OpenPages. A Natural Language Classifier service learns from your data and then can return information for texts that it is not trained on. Your administrator can link OpenPages to one or more Natural Language Classifier services, either to support different purposes or multiple languages.

**Classifier Configuration**

A classifier configuration in OpenPages defines connection information to an instance of the Natural Language Classifier on IBM Cloud. It also specifies the classifier target fields for the instance. Your administrator defines a classifier configuration.

**Classifier Field**

A classifier field is a field group in OpenPages that contains the name of a classifier configuration and a classifier input field. The **View Suggestions** button is displayed next to a classifier field.

**Classifier Input Field**

A classifier input field is a field in OpenPages that contains the text input that a Natural Language Classifier interprets and classifies. It is typically a **Description** field.

**Classifier Target Fields**

Classifier target fields are fields in OpenPages that are set when a user chooses suggestions for a classifier field.

The IBM Watson Retrieve and Rank service **helps users find the most relevant information for their query by using a combination of search and machine learning algorithms to detect signals” in the data**.

Q3.Elaborate security in smart cities.

## Securing Smart Cities

Connected smart city devices should be protected by comprehensive IoT security solutions (device to cloud). Practical and simple, yet secure, solutions that can be easily and widely adopted by OEMs and services are more effective than a ‘super solution’ that fails to gain serious traction. Such solutions should include the following capabilities:

### Firmware integrity and secure boot

Secure boot utilizes cryptographic code signing techniques, ensuring that a device only executes code generated by the device OEM or another trusted party. Use of secure boot technology prevents hackers from replacing ﬁrmware with malicious versions, thereby preventing attacks. Unfortunately, not all IoT chipsets are equipped with secure boot capabilities. In such a scenario, it is important to ensure that the IoT device can only communicate with authorized services to avoid the risk of replacing ﬁrmware with malicious instruction sets.

### Mutual authentication

Every time a smart city device connects to the network it should be authenticated prior to receiving or transmitting data. This ensures that the data originates from a legitimate device and not a fraudulent source. Secure, mutual authentication— where two entities (device and service) must prove their identity to each other—helps protect against malicious attacks.

### Security monitoring and analysis

Captures data on the overall state of the system, including endpoint devices and connectivity trafﬁc. This data is then analyzed to detect possible security violations or potential system threats. Once detected, a broad range of actions formulated in the context of an overall system security policy should be executed, such as quarantining devices based on anomalous behavior.

### Security lifecycle management

The lifecycle management feature allows service providers and OEMs to control the security aspects of IoT devices when in operation. Rapid over the air (OTA) device key(s) replacement during cyber disaster recovery ensures minimal service disruption. In addition, secure device decommissioning ensures that scrapped devices will not be repurposed and exploited to connect to a service without authorization.