50 AI Interview Questions and Answers



**Anish Mahapatra**

Contents

[List of Figures 5](#_Toc79370455)

[Introduction 6](#_Toc79370456)

[Q. What is the Gartner Hype Cycle? 6](#_Toc79370457)

[Structure of the blog 7](#_Toc79370458)

[**Part A: Topic-Based Questions** 7](#_Toc79370459)

[1 AutoML 9](#_Toc79370460)

[Q. What is Auto ML and how does it work? 9](#_Toc79370461)

[Q. What are some ways to implement AutoML? 9](#_Toc79370462)

[Q. What is transfer learning and how does it compare to a neural architecture approach? 11](#_Toc79370463)

[Q. What is GitHub’s copilot? Is it an implementation of AutoML – explain! 12](#_Toc79370464)

[Q. How does AutoML work? 12](#_Toc79370465)

[2 MLOps 12](#_Toc79370466)

[Q. What is MLOps and how does it work? 12](#_Toc79370467)

[Q. What are some of the ways to push a AI/ML model to production? 13](#_Toc79370468)

[Q. Explain how the MLOps lifecycle can be applied at an Enterprise level. 15](#_Toc79370469)

[Q. What is the difference between MLOps and DevOps? 17](#_Toc79370470)

[Q. What are the components of MLOps? 18](#_Toc79370471)

[3 AI Cloud Service 18](#_Toc79370472)

[Q. What is an API? How do we deploy our own API to productionalize a ML Model? 18](#_Toc79370473)

[Q. What are the popular Cloud Services that support AI implementations? Explain! 19](#_Toc79370474)

[Q. What Cloud Service would you prefer? Why? 20](#_Toc79370475)

[Q. What are some scenarios where AI Cloud Service could be used to increase ROI? 21](#_Toc79370476)

[Q. What are the benefits of Machine Learning on the cloud? 21](#_Toc79370477)

[4 NLP: Natural Language Processing 21](#_Toc79370478)

[Q. What is NLP? Explain the components of NLP? 21](#_Toc79370479)

[Q. What are chatbots? What are the various implementations of chatbots used? 22](#_Toc79370480)

[Q. What are the main issues faced by companies when implementing chatbots? 23](#_Toc79370481)

[Q. Explain some NLP use-cases. 23](#_Toc79370482)

[Q. How does Transfer Learning aid in building better and faster NLP models? What are the top three most popular implementations of pretrained language models? 24](#_Toc79370483)

[5 AI Governance & Scalable AI 24](#_Toc79370484)

[Q. Now that large companies are leveraging AI to make decisions that affect human beings everyday, it is important to critique the algorithms implemented. On that note, what is AI governance? 24](#_Toc79370485)

[Q. What are the components of AI Governance? 25](#_Toc79370486)

[Q. Good AI exists. Looking at the top companies in the world, we know that a robust framework exists where AI can scale. How do the best companies in the world build Scalable AI? 26](#_Toc79370487)

[Q. What are the difficultes when it comes to scaling implementations of AI? 28](#_Toc79370488)

[Q. State out the Enterprise AI Journey. 29](#_Toc79370489)

[6 XAI / Explainable AI 30](#_Toc79370490)

[Q. What are some of the common problems faced by companies when it comes to interpreting AI / ML? 30](#_Toc79370491)

[Q. Explain the concept of XAI and how it can be used in real world implementations? 31](#_Toc79370492)

[Q. If we were to consider AI/ML Models as black boxes that give us the desired output, what are some of the ways to help being trust back to the models being leveraged? 32](#_Toc79370493)

[Q. Explain some examples of tools and technologies that can help implement interpretable machine learning or XAI. 33](#_Toc79370494)

[Q. All of the conversations about XAI seem to be problems of the future. If you were to design a AI / ML model for a business now and productionalize a model, what are some of the considerations you would have as a lead of the project? 34](#_Toc79370495)

[7 Ethical AI / Federated Learning (TBD) 35](#_Toc79370496)

[Q. With a world being driven more towards a privacy-focus mentality, what are some of the recommended approaches companies / teams can take to ? 35](#_Toc79370497)

[Q. A common statement is “With the onset of the Digital Era”. In the coming years, as AI startes to take over more and more components of human life, the statement is going to transition to “With the onset of the AI era”. Is Ethical AI a real concern or just hype? What are the ramifications? 35](#_Toc79370498)

[Q. How can Ethical AI be implemented at an enterprise level? What are its implications for Enterprise AI use-cases and Governance? 35](#_Toc79370499)

[Q. With privacy focus coming to the forefront, a lot of attention has been brought on data collected. A new branch of data collection and processing for ai / ml is federated learning. Explain further. 35](#_Toc79370500)

[Q. Explain how a model can be monitored after it is moved to production. Break down the approach. 35](#_Toc79370501)

[8 Cyber Security AI 35](#_Toc79370502)

[Q. Cybersercurity is the need of the hour. What is a good way to classify all security-related tasks using the PPDR framework? 35](#_Toc79370503)

[Q. How can machine learning be used within the space of Cyber Security. Broadly explain the various elements of Cyber Security. 36](#_Toc79370504)

[Q. Mention ten use-cases as to how AI / ML can be used within Cyber Security use-cases. 37](#_Toc79370505)

[Q. Explain the flow of Cyber Security attacks and how AI / ML models can help plug the gaps. 38](#_Toc79370506)

[Q. How can Cyber Security be implemented across a PoC Team or at an enterprise-level with the help of AI / ML? 38](#_Toc79370507)

[9 RPA: Robotic Process Automation 39](#_Toc79370508)

[Q. What is Robotic Process Automation? Explain in brief with a few examples. 39](#_Toc79370509)

[Q. What is the difference between AI and RPA? 40](#_Toc79370510)

[Q. Explain the landscape of how RPA and AI can be used in tandem to increase revenue at an enterprise-level? Discuss a few use cases. 41](#_Toc79370511)

[Q. What are the phases of RPA at an Enterprise Level? 41](#_Toc79370512)

[Q. Why are people doing RPA? Is it actually worth pursuing? 42](#_Toc79370513)

[10 GANs: Generative Adversarial Networks 43](#_Toc79370514)

[Q. What are GANs? 43](#_Toc79370515)

[Q. Provide an overall system view of GANs. 43](#_Toc79370516)

[Q. Explain some uses-cases on the variations of GANs. 43](#_Toc79370517)

[Q. Name some popular tools used for GANs. 43](#_Toc79370518)

# List of Figures

[Figure 1 The AI Hype Cycle (Source: Gartner) 9](#_Toc79274700)

[Figure 2: Data Science is a subset of Artificial intelligence 10](#_Toc79274701)

[Figure 3: AutoML Workflow 11](#_Toc79274702)

[Figure 4: The end to end MLOps Lifecycle (Image by seldon.ai under the CC BY-SA 4.0) 15](#_Toc79274703)

[Figure 5: End to End ML Workflow (Source: ml-ops.org) 16](#_Toc79274704)

[Figure 6: Model Serving (Source: ml-ops.org) 17](#_Toc79274705)

[Figure 7: MLOps: The AI Lifecycle for IT Production 18](#_Toc79274706)

# Introduction

With so many pseudo-data scientists cropping up due to numerous courses that offer theoretical learning, the questions in interviews are getting streamlined to filter those that understand how real-world implementation works. It is important to understand how data flows in the real world and what sort of questions are being discussed across companies.

**The value of a company lies solely in the interview process.**

Interviews across companies are growing to appreciate those that have an end-to-end understanding of how problems can be dealt with over theoretical understanding. This detailed blog is dedicated to helping you understand the latest trends in the industry and how you can absorb them. Everything you will need to know for an interview will be detailed out here. We will start off by understanding what the trends in artificial intelligence are.

## Q. What is the Gartner Hype Cycle?

Gartner is a market leader in market research. The Gartner Hype Cycle Methodology is an industry-approved representation of how a technology or application will mature over time. It represents initial interest, a peak in its hype, rolls down to reduced interest in the technology followed by maturity and implementation. A lot of demand in the market comes through in two points in this cycle, in the peak and the maturity. That's where most of the money can be made from a corporate job.

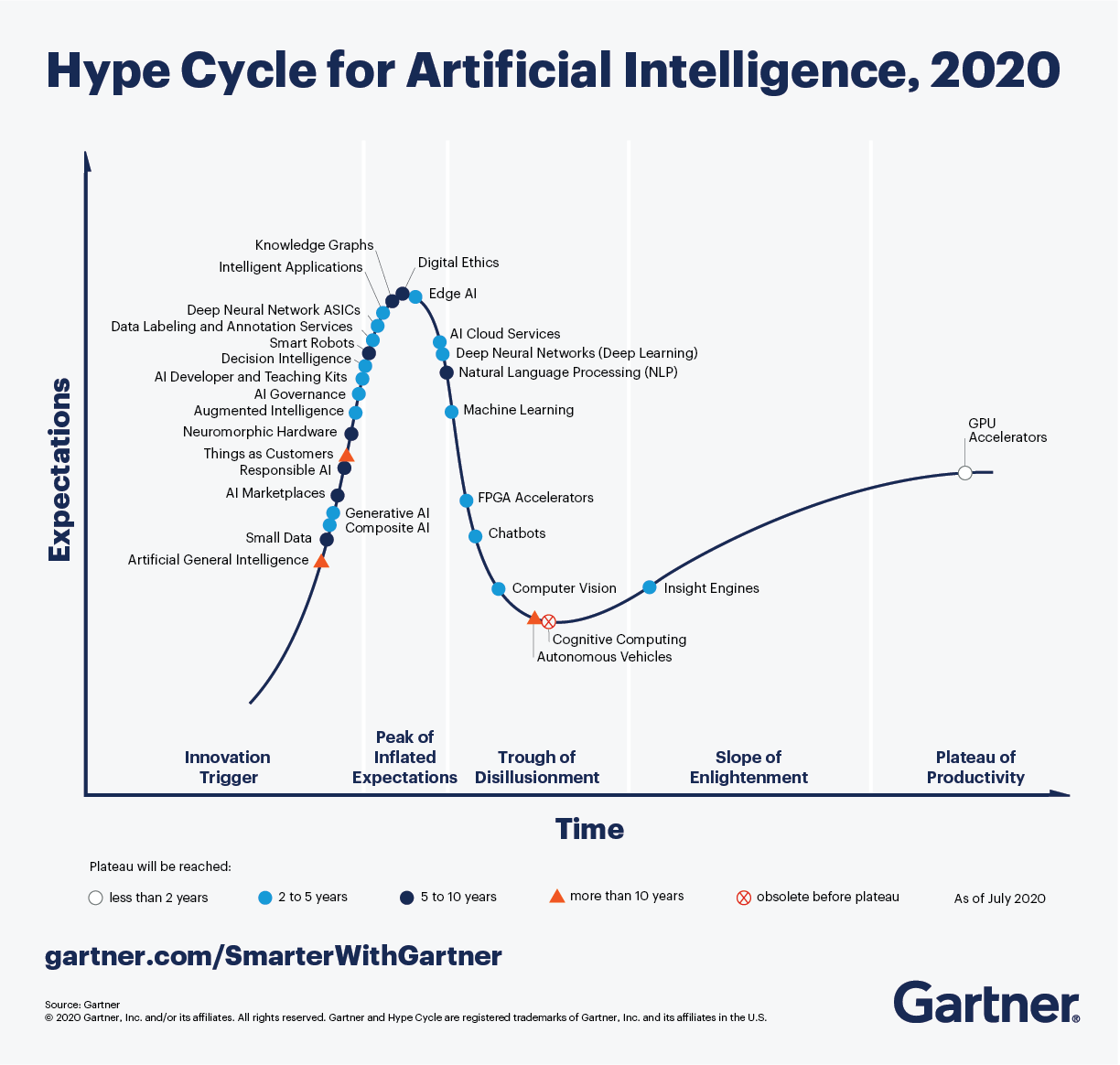


Figure 1 The AI Hype Cycle (Source: [Gartner](https://www.forbes.com/sites/louiscolumbus/2020/10/04/whats-new-in-gartners-hype-cycle-for-ai-2020/?sh=fe3826f335c4))

Looking at the Hype Cycle for artificial intelligence, focusing on the **blue** dots in the cycle, those are topics that are of interest in the next two to five years. An understanding of various innovation triggers in the space of artificial intelligence will help elevate the conversation and make you stand out in the eyes of the interviewer. The answer is never to simply answer the question but add an additional layer of context that will stick.

This blog will not tell you exactly how to answer questions when asked. It will explain what an instance of the best-in-class answers would sound like. We will try to use as many visual aids and examples to answer so that you can apply them in multiple scenarios and interviews.

# **Part A:**

Before we deep-dive into the questions below, let's understand more about artificial intelligence and where it falls in the spectrum. In the recent past, Data Science has taken off in the space of technology, even being crowned as the Sexiest Job of the 21st Century. Let's understand where Data Science belongs in the space of Artificial Intelligence.

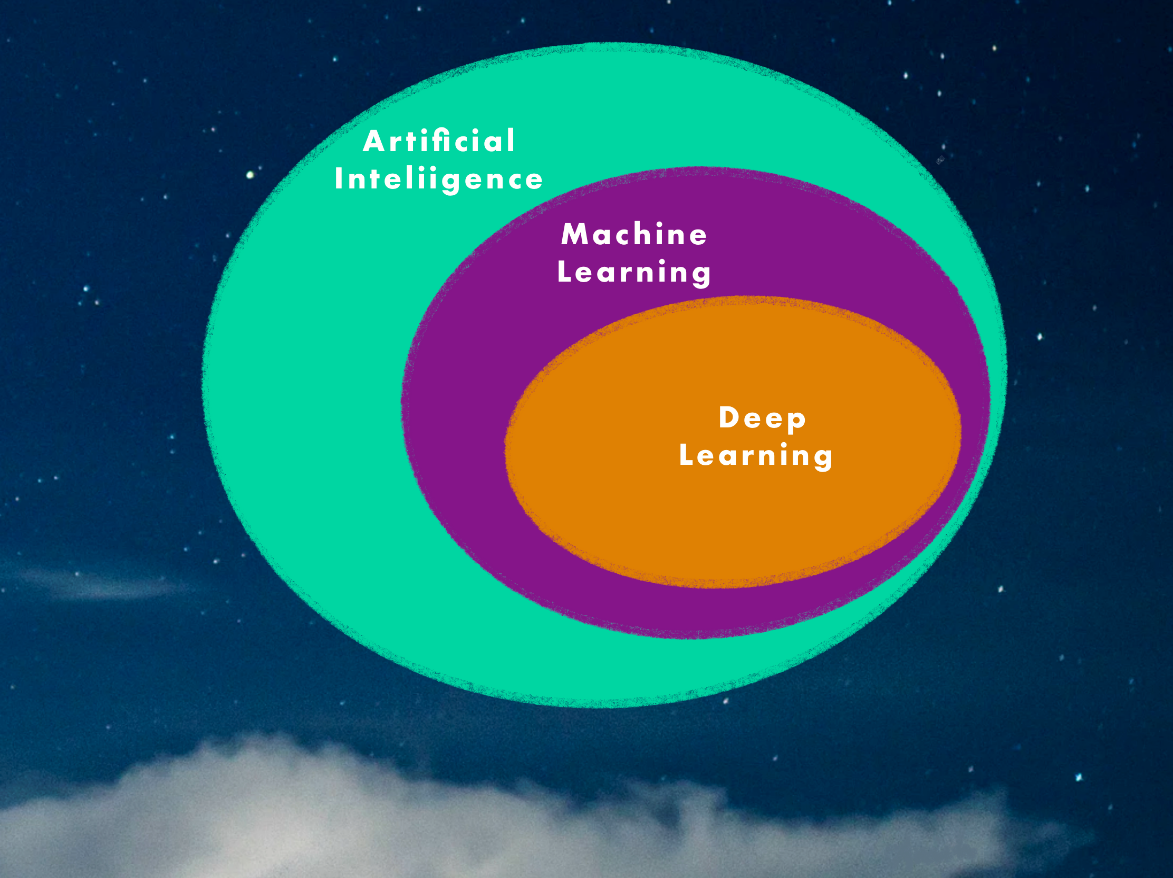


Figure 2: Data Science is a subset of Artificial intelligence

* **Deep Learning**: Subset of machine learning that leverages neural networks to train itself to perform layered tasks such as speech and image recognition
* **Machine Learning**: Subest of Artificial Intelligence which enables algorithms to learn without being explicitly programmed
* **Artificial Intelligence**: Programs with the ability to learn and reason like human beings

When explaining questions to an interviewer, remember, they are smarter than they look. No one knows everything about any topic, especially in a subject like Artificial Intelligence, where new things are coming up at an exponential rate. When answering questions, be humble and truthful. If you know the answer to the question, answer confidently. If you are unsure, be vocal about your thought process and the way you are thinking – take inspiration from the examples below and explain the answer to the interviewer through your experiences from projects and learnings. So right before we start, I would like to let you know that the focus of this blog is to get you started for interviews and give you exposure to what is the latest in the field of Artificial Intelligence. Consider all of the answers as one way to go about it, and please feel free to pitch in your thoughts as well. Alright, we have had enough fun building up to this moment. Let's dive right into the questions!

# 1 AutoML

## Q. What is Auto ML, and how does it work?

A. So, for anyone who has heard or worked on a traditional machine learning flow, we know that a traditional machine learning flow goes from Data Acquisition to Predictions. The following diagram explains Auto ML.

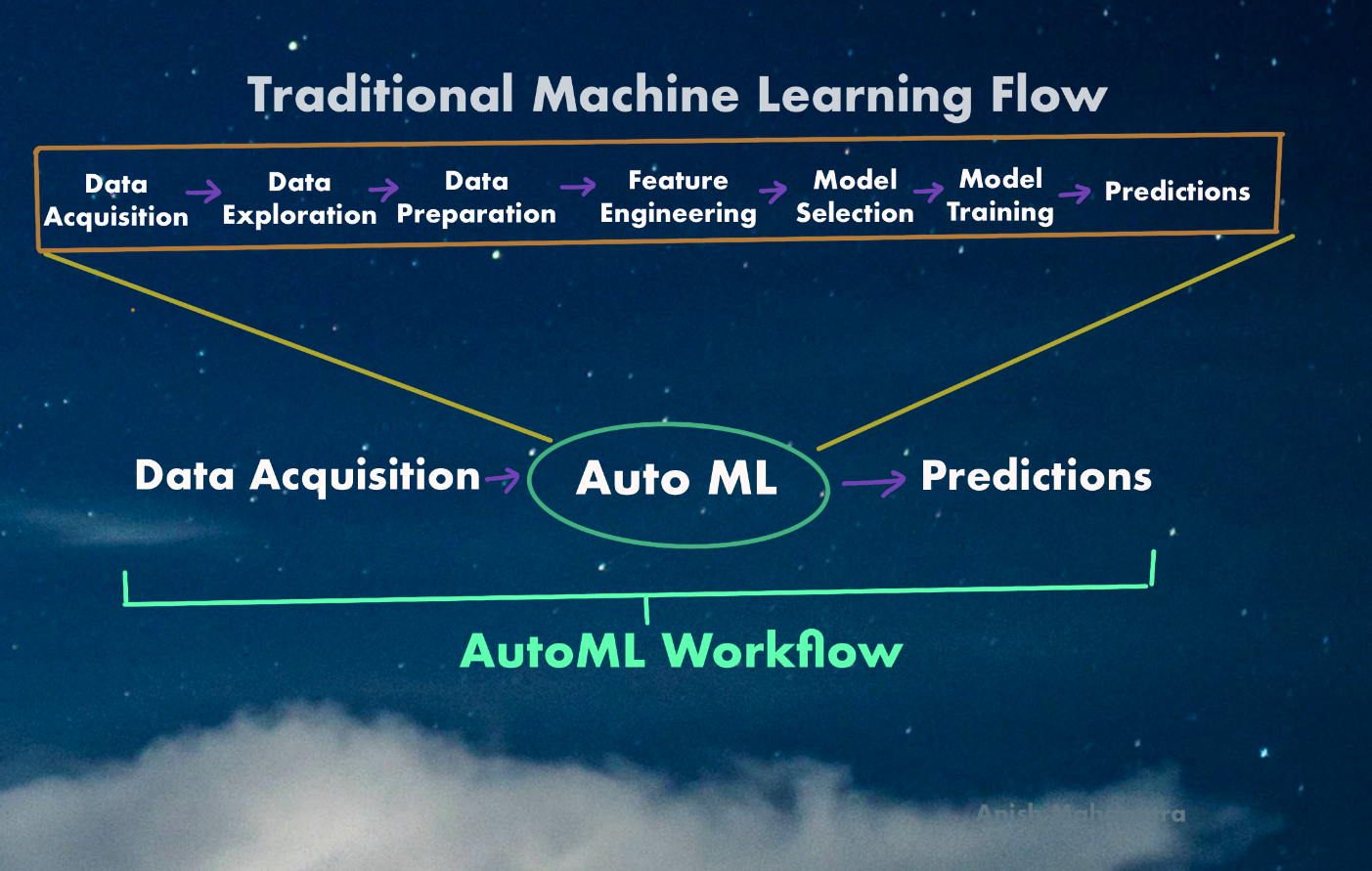
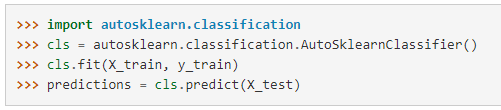


Figure 3: AutoML Workflow

As a Data Scientist, numerous activities go into the traditional machine learning flow. The process of automating the tedious, iterative tasks in the development of machine learning is known as AutoML. The benefit of AutoML is that it is a low-code or no-code approach, wherein folks who do not have experience in Machine Learning can also implement it.

## Q. What are some ways to implement AutoML?

A. Following are some of the popular ways to implement AutoML:

* **Auto-SkLearn**:   
  Scikit-learn is a package that every data scientist has used. Auto-sklearn is an automated machine learning toolkit that does that same thing except that it is an automated replacement for a sci-kit learn estimator.   
    
  The estimator automatically performs the algorithm selection as well as the hyperparameter tuning
* **Auto-Keras**:   
    
  To recall, Keras is an open-source library that provides a Python interface into the world of Artificial Intelligence, especially Tensorflow. AutoKeras is the AutoML system that is based on Keras. AutoKeras focuses on making machine learning and deep learning easier with the help of Neural Architecture Search. This will help non-coding folks achieve the state of the art performance with minimal coding effort.
* **Auto-Weka**:  
    
  Weka is an extremely popular java-based machine learning software for data exploration. Similar to other AutoML applications, AutoWeka considers all possible algorithms and even applies hyperparameter tuning to be able to select the optimal fit using the latest strides in Bayesian Optimization.
* **Amazon Lex (Amazon)**:   
    
  Consider Amazon Lex as the AutoML backend of the extremely popular Amazon Alexa. With features such as Automatic Speech Recognition (ASR) and Natural Language Understanding (NLU), if you are building a chatbot, this is a great toolkit.
* **Azure ML Studio (Microsoft)**:   
    
  With Azure ML Studio, Microsoft provides an AutoML application with a Graphical User Interface and Drag & drop format to try multiple algorithms along with hyperparameter tuning. It has automated components of the traditional ML Flow from data acquisition, experimentation and even logging—definitely, a must-try within the Azure ecosystem.
* **Vertex AI (Google)**:   
    
  Google recently (May 2021) launched a unified AI platform to build, deploy and scale machine learning models for individuals as well as enterprises. This AutoML application also includes MLOps tools to manage data and models at Scale. For the entire ML Workflow, Vertex AI is a one-stop shop for an end to end integration of AI that supports all open source frameworks.
* **H20AutoML**:   
     
  Anyone who has attempted to work on AutoML in the past decade has heard of H20.ai. H20AutoML is H20.ai's foray into the space of AutoML. It is a function with the goal of finding the best model with minimal knowledge or effort from the Data Scientist.

## Q. What is transfer learning, and how does it compare to a neural architecture approach?

A. Transfer learning is a process wherein the learning from an already developed model is resued and built upon for a new task. Essentially, it is using pre-trained models and customising them for your use case.

**Transfer Learning versus Neural Architecture Search**

The premise of transfer learning is that neural networks generalise and converge when it comes to similar use-cases. For example, boxes, squares, rectangles and crystals are similar in nature. This assumption allows us to build more on top of these generalisations for specific use-cases.

Neural Architecture search, on the other hand, is based on the premise that each use case is unique and should be done up from scratch. This novel architecture with its own hyperparameters will perform the best. However, the disadvantage is that we will also have to train from scratch, and pre-trained models cannot be used.

A quick note here – Google's latest AutoML products subscribe to the school of thought that the neural architecture search needs to be used directly for the most optimal approach. This is an area that is still being explored, and with progress in AutoML, we will learn more.

## Q. What is GitHub's Copilot? Is it an implementation of AutoML – explain!



GitHub is the go-to website for source code management. GitHub copilot is an AI tool developed collaboratively by GitHub and OpenAI to assist users by autocompleting code. Copilot is set to be an extension for MS Visual Code that not just autocompletes a few functions or phrases, but entire functions! This is an extension of pair programming, where two programmers work on the same set of code to speed up the development process. It was trained on all available open-source code and is powered by a deep neural network language model called Codex.

Since GitHub copilot still aids the developer in auto-completing code, it would not classify completely as AutoML in its current state, in my opinion. However, as the project progresses and moves out of the *preview* stage, GitHub Copilot can be the gold standard of AutoML tools.

## Q. How does AutoML work?

A. If you have ever automated anything, pipelines are the best way to automate and orchestrate workflows. AutoML is essentially a set of automated pipelines, that when triggered, simply try out all the permutations and combinations until they come up with the top results.

This would include the automation of a standard machine learning workflow which would include the steps of

* Gathering the data
* Preparing the Data
* Training
* Evaluation
* Testing
* Deployment and Prediction

This includes the automation of tasks such as Hyperparameter Optimization, Model Selection and Feature Selection. The orchestration of pipelines can happen on various platforms but are generally integrate with cloud providers such as Microsoft Azure, Amazon Web Services or Google Cloud Platform at an Enterprise Level.

# 2 MLOps

## Q. What is MLOps, and how does it work?

A. If you have worked on machine learning projects and proof of concepts (PoC), you must have realised that a lot of AI / ML models end up not going into production, and hence, do not make generate any revenue for the stakeholders. This is the main reason why projects are short-lived, and there is so much experimentation that does not lead to desired results.

MLOps is an end-to-end machine learning development process that aims to design, build and manage reproducible, scalable and evolvable ML-powered software. It is the perfect culmination of software engineering into machine learning so that the outcomes of machine learning are products that can scale.

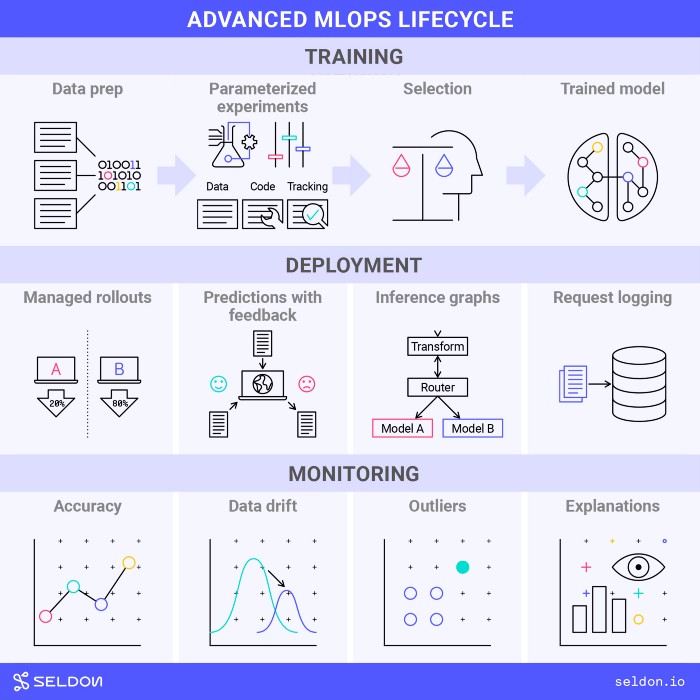


Figure 4: The end to end MLOps Lifecycle  
(Image by seldon.ai under the [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/))

A classic example of how MLOps can be broken down into an ideal MLOps Lifecycle has been given above, which consists of training, deployment and monitoring.

## Q. What are some of the ways to push an AI/ML model to production?

When a model is in the prototype and development phase, a lot of teams use IDEs such as Jupyter Notebook. While this might seem like the best option during development as we are able to see the results instantly, it is advisable to write code that is worthy of being moved into production. The entire cycle can be visualised as shown below.



Figure 5: End to End ML Workflow  
 (Source: [ml-ops.org](https://ml-ops.org/content/end-to-end-ml-workflow))

Now, let's discuss how AI / ML models can be deployed into production. The ideology behind all of the steps is **pipelines**! Experiment to see what works best for your data, automate it using pipelines and then monitor the performance of the workflow.

* **Data: Data Engineering Pipelines**Data is everything. Make sure that the quality of data works for your use case.
  + Data Ingestion
  + Exploratory Data Analysis (using RAD Tools)
  + Validation
  + Data Wrangling
  + Data Splitting
* **Model: Machine Learning Pipelines**Every team enjoys experimentation with data. It is important to also be transparent with the business during the phase of documentation and also give equal focus to logging all experiments & learnings.
  + Model Training
  + Model Evaluation
  + Model Testing
  + Model Packaging
* **Code: Deployment Pipelines**   
  Once the final ML model has been decided, it is critical for the model to be pushed into production. This would include the following phases:
  + Model Serving
  + Model Performance Monitoring
  + Model Performance Logging

Based on demand, the model serving requirements can be further analysed.

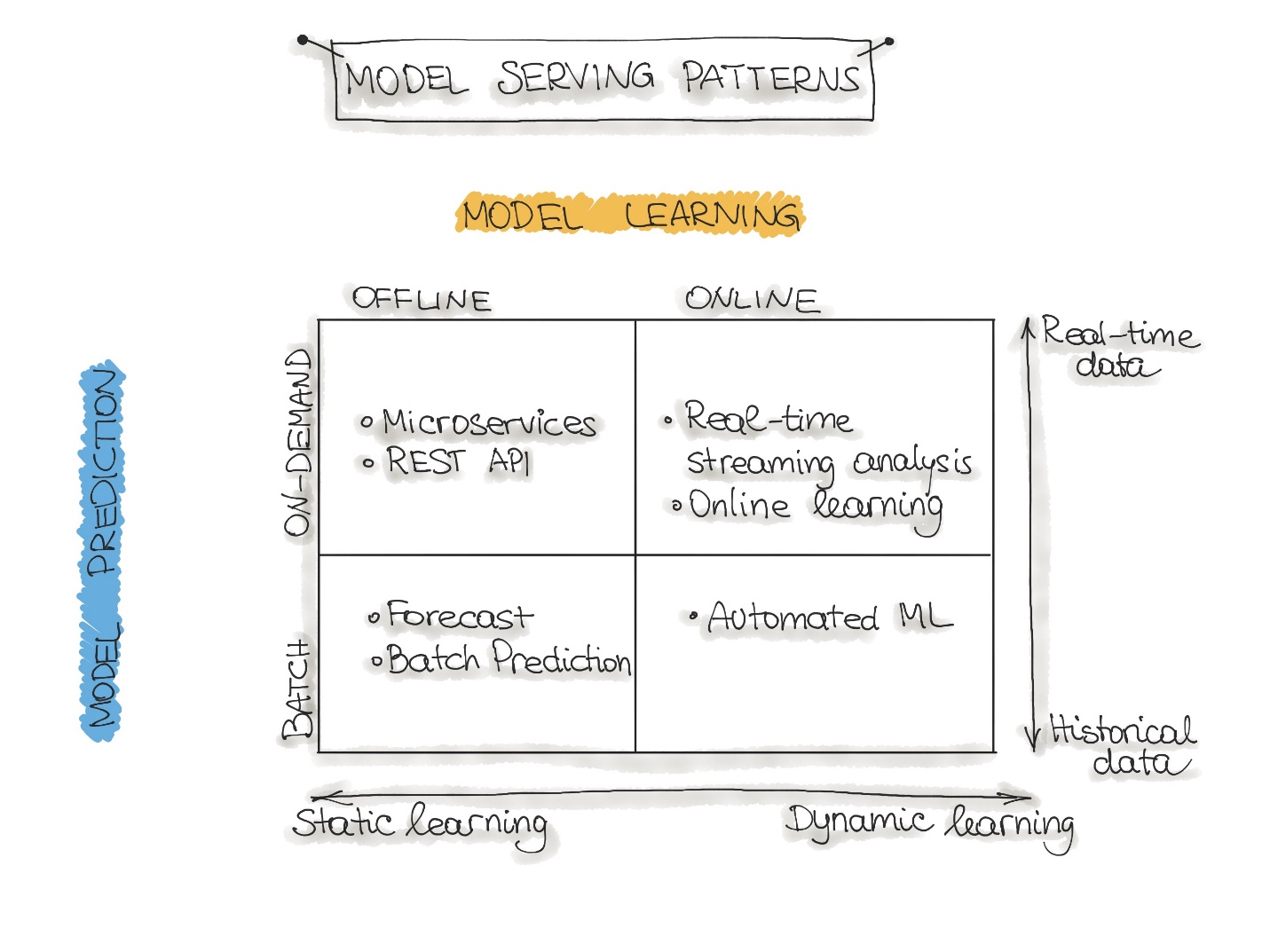


Figure 6: Model Serving  
(Source: [ml-ops.org](https://ml-ops.org/))

## Q. Explain how the MLOps lifecycle can be applied at an Enterprise level.

For Machine learning models to go into production, we need to stop thinking of machine learning as strictly iteratively experimental. MLOps is the marriage between machine learning and software engineering. The final output should be visualised as a product. So, when a technology product is being developed, the code needs to be functional, modular and tested.

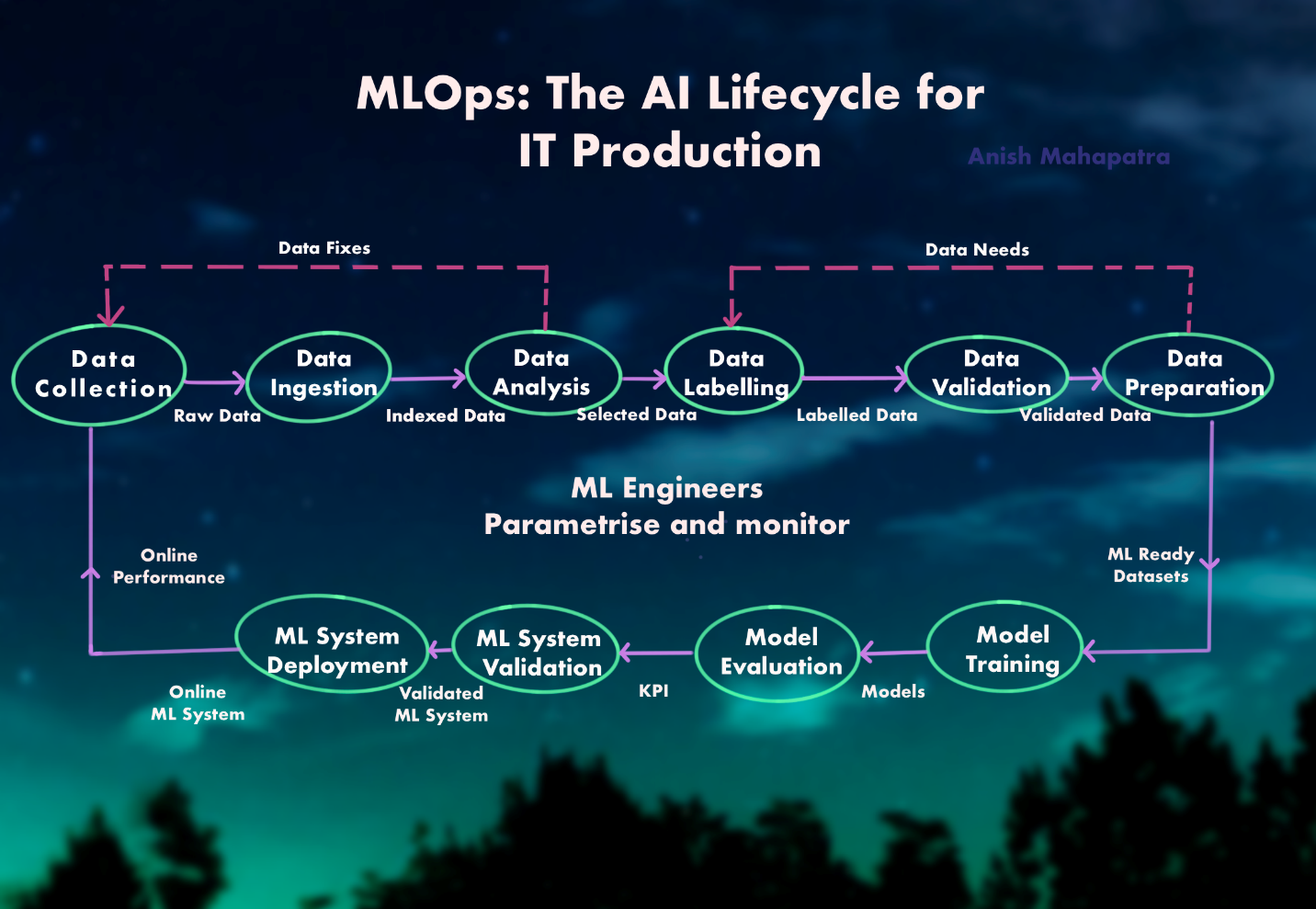


Figure 7: MLOps: The AI Lifecycle for IT Production

MLOps follows a similar lifecycle as a traditional machine learning flow except that the model continues in the workflow to production. This is then monitored by MLOps Engineers to ensure that the quality of the model in production is as expected. In terms of the tools used in MLOps, here are a few use-cases.

* **Model Registries**   
  This is what it sounds like. Model Registries larger teams keep track of version models and store them. It is even possible to revert to an older version
* **Feature Stores**   
  When experimenting with larger sets of data, there might be various versions of the analytical datasets and subsets for different tasks. A feature store is a modern, elegant solution to leverage data prep work from previous runs or other teams as well
* **Metadata Stores**   
  For unstructured data such as image and text data to be leveraged effectively, it is important to track metadata effectively in the production

## Q. What is the difference between MLOps and DevOps?

DevOps is a set of practices used across enterprises to reduce the software development lifecycle. It provides a continuous integration and continuous development (CI/CD) approach to the software development lifecycle.

**Highly Experimental**   
While DevOps works in an environment that is more application and optimisation oriented, machine learning systems are highly experimental in nature. Thus, MLOps needs to take into account various experiments, feature engineering, model parameters, model tuning etc.

**Testing**   
MLOps goes beyond unit testing. Model KPIs such as data quality parameters, model drift, model bias and performance needs to be tracked

**CACE Principle**   
MLOps follows the CACE Principle – **C**hange **a**nything, and it **C**hanges **e**verything. Machine learning systems are highly dependent on the nature of the problem and the data in consideration.

**Deployment**   
Deployment for machine learning systems involves multiple steps such as data processing, feature engineering, model training, model registry and model deployment. DevOps follows a CI/CD approach, but in MLOps, there is an additional concept of Continuous Training (CT)

**Tracking Lifecycle**   
In DevOps, tracking the performance of the code is sufficient. In MLOps, it is necessary to track the data quality parameters through every step in the workflow as well

## Q. What are the components of MLOps?

There are a few ways to break down this question. One way that MLOps can be broadly broken down is:

* **Design**   
  Design thinking plays a big role in MLOps. All the way from the nature of the problem, the hypotheses to be tested, the architecture and the deployment
* **Model Development**   
  This phase includes the data engineering pipelines, the experimentation to get the suitable machine learning systems in place and model testing & validation
* **Operations**   
  As part of the operations, the model has to be deployed, tested and analysed over time. The CI/CD pipelines are triggered using an orchestration tool and monitored.

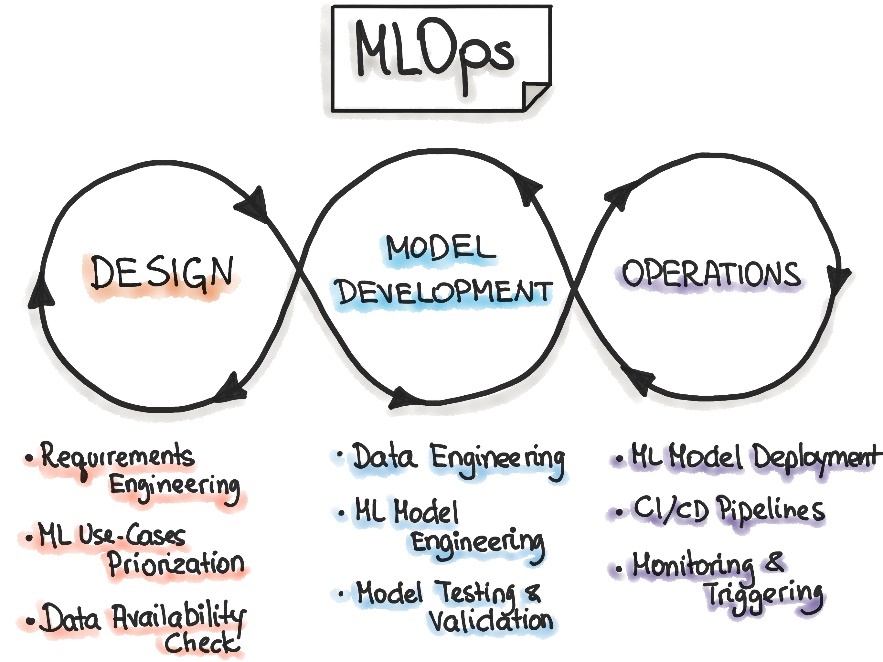


Figure 8: Components of Machine Learning  
(Source: [ml-ops.org](https://ml-ops.org/))

# 3 AI Cloud Service

## Q. What is an API? How do we deploy our own API to productionalize an ML Model?

A. Most Data Scientists know how to run python code on a Jupyter Notebook. We run the codes, do data analysis, come up with the final model result and stop there. How do machine learning systems in the real world interface with the rest of the systems in place? Even though python is great to experiment and perform machine learning, in terms of deployment, there are two main options:

* **Rewrite the logic** in a language that fits into the technology stack being leveraged   
  Imagine going through the entire machine learning workflow only to have to do it again. This is an option I would not recommend as the return on investment is not worth it.
* **API-first approach**Okay,so how do applications that use different frameworks or languages cross-communicate? APIs! APIs help cross-language applications function efficiently. So, what if you made the final machine learning model that makes sense, and you create a sort of endpoint that other developers or the front-end team can connect to. All they would need is the URL endpoint from where the API is being served.

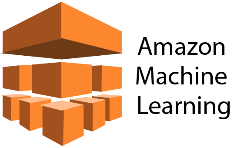
API – Application Programming Interface help applications talk to each other. The person who needs to connect to the API needs to perform a simple REST call to the API using a Software Development Kit (SDK).

The two more popular approached to productionalizing our machine learning models is using Flask or FastAPI. So, basically, we serialise/deserialise the machine learning model objects into a pickle (.pkl) or an h5py file, and we let users query it.

Think about it this way, let's say we are deploying a model that predicts the probability of churn for a customer. So, if the query were a new customer, then the returned results would be the probability, which we could configure in the front end to say *churn* or *no-churn* based on the threshold.

## Q. What are the popular Cloud Services that support AI implementations? Explain!

A. AI Implementation is a fancy way of saying, are you able to handle an end to end implementation of AI / ML models on the cloud? To understand further, it is a good idea to get familiar with the term MLaaS, which is Machine Learning as a Service. MLaaS offers multiple ML related services as an additional component to cloud computing. There are multiple options in the market, so it would depend on the use-cases being tackled. Let's discuss a few of the popular ones:

* **Google's Vertex AI**   
     
  Google recently unveiled their Unified MLOps & AI Platform – Vertex AI to help Data Scientists / ML Engineers increase experimentation, deploy faster and manage models better
* **AWS Machine Learning**   
    
  AWS is the largest player in the cloud computing market. Their Machine Learning offerings have matured over time to cater to all machine learning needs from speech recognition, computer vision, AI etc.
* **Azure Machine Learning**   
    
  Azure has been grabbing more market share over the years because it has been doing a lot right in the machine learning space. Azure Machine Learning is a no-code, drag and drop interface to perform machine learning at Scale along with model management.

## Q. What Cloud Service would you prefer? Why?

This is a critical thinking question. It relies on your understanding of the use-case, cloud services and confidence in implementing scalable solutions. Probe more into the functionality or use-case the interviewer is asking. There are multiple factors one can consider:

* Is the existing data on on-prem servers or already on a cloud platform?
* Does the team already use an existing AI Cloud Service Provider?
* What is the skillset of the team on the cloud platform?
* What is the nature of machine learning being performed?
* What sort of architectural needs will the project have, and what are the associated costs?
* How future-proof are the project and the platform?

Objectively, if we are comparing platforms, GCP is ahead of AWS and Azure. AWS is difficult to configure and set up – it is confusing for beginners and is comparatively complicated.

Azure is good for basic functionalities, but there is a lot Azure needs to mature over in terms of Machine Learning. GCP is new, and so uses the latest tech stack. Everything is bleeding edge, plus there is nobody that does Machine Leaning like Google, so the entire cloud computing stack is machine learning focused.

A few more tangible points why GCP is better:

* A lot of Google's work is open-source
* Their Speech and Translate APIs are market leaders in their respective segments
* AutoML is pretty great for multiple use-cases
* They have custom-designed ASICs called TPUs for optimised workloads

## Q. What are some scenarios where AI Cloud Service could be used to increase ROI?

A. Some scenarios where AI Cloud Services can be leveraged are:

* **Customer Service Automation**: Integrating Machine Learning and speech recognition into customer service can help save a lot of overhead costs
* **Personalisation and Engagement**: Tailoring personalised customer experiences can lead to better sales and happier customers, which in turn leads to a higher revenue
* **Fraud Detection**: Multi-touch fraud detection algorithms can help isolate and pick out points where gaps can be plugged
* **Scalable Media**: Scalable architecture can be leveraged based on the number of concurrent users and workload
* **Forecasting**: Multiple decisions can be optimised by leveraging accurate forecasting in terms of sales, supply-demand, costing, dynamic pricing etc.

## Q. What are the benefits of Machine Learning on the cloud?

For use-cases that need both proofs of concepts or scalable solutions, working on the cloud can have multiple advantages. Some of the benefits are listed below:

* **More Economical**   
  Working in a pay-per-use model has numerous cost benefits that can be passed on to the business. The cost of maintaining and upgrading legacy hardware is also eliminated
* **Less configuring**   
  One of the most time-consuming aspects is to configure and set up the same set of applications across multiple hardware touchpoints. This needs to be kept track of, along with security and updates. The advantage of working on the cloud is that everything is handled by the experts for a reduced cost as a result of economies of Scale
* **Elastic Architecture**Whether you need 1/10th of your existing needs or 1000 times more. Both can be done with cloud architecture with the click of a button
* **Better support for streaming architectures**   
   With real-time analysis taking the forefront where multiple consumers are getting used to things being done instantly, there is much greater support for real-time or in-time architectures as compared to on-prem settings.

# 4 NLP: Natural Language Processing

## Q. What is NLP? Explain the components of NLP?

Human language is spread with intricacies that make it complicated to decipher. Obtaining intended meaning from speech or text is even more difficult, especially when software is used. Natural Language Processing (NLP), a part of Information Retrieval, breaks down speech and text to help software understand what is happening.

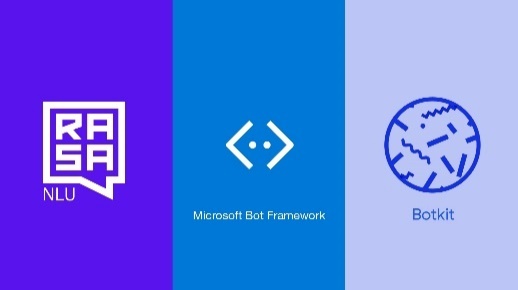
The components of NLP are as follows:

* **Speech Recognition**Recognising speech and being able to convert it reliably to text. There are various components of speech itself along with multiple accents globally, which makes this a challenge
* **PoS Tagging**Differentiationof the parts of a sentence to help tag the parts of speech such as noun, verb, adjective etc.
* **Word sense disambiguation**Semantic analysis to determine the right meaning of the word being used
* **Naming Entity Recognition**Identify proper nouns as entities as a part of the sentence such as name, location etc.
* **Co-reference resolution**Identify if pronouns refer to the same object. For instance, the question "*How old is Obama?"* And the follow-up question of *how tall is he?* should provide the right answer if the co-reference resolution is configured correctly
* **Sentiment Analysis**Understanding the tone of the speech or text based on subjective qualities or words used. This is used in social media to better gauge sentiments towards an event or a product.
* **Natural Language Generation**This is giving power to the algorithm to make sentences that would make sense to humans. This is currently a hot area of research along with NLU (Natural Language Understanding)

## Q. What are chatbots? What are the various implementations of chatbots used?

Chatbots are the medium through which NLP is carried out. A chatbot is a software that simulates human-like conversations to enable users to do tasks that can be automated. Chatbots can help businesses generate revenue by reducing the human effort to do repetitive tasks and even generate sales by interacting with potential leads.

The popular implementations in the market are:

* **Google's Dialogflow**   
    
  Google is great at speech and natural language processing. Dialogflow grants enterprise users access to all of Google's tremendous Speech APIs that can be integrated within various platforms
* **Facebook's wit.ai**   
    
  With Facebook owning platforms such as Facebook, Instagram and WhatsApp, facebook's reach in marketing is tremendous. Wit.ai is Facebook's NLP offering to enable users to integrate the chatbot with multiple applications to aid for an enhanced experience.
* **Microsoft's BotKit**   
    
  Botkit integrate seamlessly into Microsoft's ecosystem with a support framework that can support a host of applications such as Teams, messenger, Slack, Telegram etc. and can be automated as well
* **Rasa**   
    
  Rasa is an open-source framework to tackle the best problems in NLP, NLU. It is made for personalised conversations at Scale

## Q. What are the main issues faced by companies when implementing chatbots?

When chatbots are to be implemented atop existing tech stacks, the following are a few of the common issues seen across clients:

* Compatibility with an existing technology stack
* Security vulnerabilities (as chatbots have to query sensitive datasets)
* Transparency and visibility into end to end implementation
* Implementation at Scale along with the growth of the business
* Future-proofing AI implementations
* Return on Investment

A use-case I have come across when Fortune 500 clients inquire about chatbots is whether it is possible to perform everything without the intervention of third parties such as Google, Facebook and Microsoft. So, Rasa gets recommended a lot as it can even work without the internet (locally), and it integrates just as easily with a larger set of applications at multiple levels.

## Q. Explain some NLP use-cases.

Some of the popular use-cases of NLP are explained below:

* **Understanding customer sentiment**: Analysing multiple touchpoints to understand the pain points of customers can lead to quicker, more accurate resolution. This reduction in friction can lead to higher sales.
* **Multi-lingual Support**: As businesses go global, reducing the barrier of language with the help of multi-lingual support can play a big role in scaling companies and products
* **Entity Extraction**: Understanding the relevant parts of the sentence along with intent classification can aid in analysing specific demographics
* **Automation of receipt and invoice processing**: Automation of invoice processing with the help of textual analysis and fraud detection can help reduce operational costs tremendously
* **Content classification**: Classification of inappropriate content can save companies cost and time. Classification of relevant content in a domain-specific manner can help build contextual relationship graphs

## Q. How does Transfer Learning aid in building better and faster NLP models? What are the top three most popular implementations of pre-trained language models?

Training NLP models takes time. Imagine training a model of the complete context of human language. So, it only makes sense that we should be able to reuse the training rather than try to train from scratch every single time. That is what transfer learning achieves.

Transfer learning is building on existing training to train and build towards another use case. It is building a more specific context over a generalised context. Three of the most popular NLP implementations are as follows:

* OpenAI's GPT-3 (Generative Pre-Trained Transformer 3): The implementation of GPT-3 has been pegged as a revolution in NLP. It has achieved a God, cult-level status as the best implementation of NLP to date. However, due to its limited availability, it is yet to be tested by the general public. We have had the chance to see a few use-cases, and the results look unbelievably positive
* BERT (Bidirectional Encoder Representations from Transformers): BERT is designed to pre-train deep bidirectional representations. BERT is conceptually simple and empirically powerful
* XLNet: XLNet is a generalised autoregressive pretraining method that leverages the best of both autoregressive language modelling (Transformer-XL) and bi-directional capability (BERT)

# 5 AI Governance & Scalable AI

## Q. Now that large companies are leveraging AI to make decisions that affect human beings every day, it is important to critique the algorithms implemented. On that note, what is AI governance?

There are still people who still believe AI is the future. The truth is the AI age is fully here and is becoming more prominent every year. A good point of view to discuss for this question is a recent article by Bloomberg [Fired by Bot: Amazon Turns to Machine Managers, And Workers Are Losing Out - Bloomberg](https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out) where algorithms are terminating contract drivers when they are not even at fault.

There are AI / ML algorithms that analyse the path the delivery drivers take, the time taken to delivery, customer satisfaction scores and a host of other factors and rate the performance of the driver. Amazon is a company that functions optimisation, so they have replaced an entire HR Team with algorithms. This trend is worrying, especially if transparent policies to give visibility into end to end reasoning is not provided. AI Governance is a necessary evil. Without it, the very pillars of society can break down.

The four guideposts of AI Governance are as follows:

* **Integrity**   
  The integrity and validity of the algorithm has to be justified by analysing decision lineage and justification of what micro-decisions lead to the final output
* **Explainability**   
  End to end transparency of the process can help stakeholders understand not just the decision but also the reasoning behind it
* **Fairness**   
  Bias is an impending issue in most machine learning systems. Bias can be due to the data or algorithmic as well. It is on AI Governance to ensure that AI Systems are ethical, non-prejudiced and protected against bias
* **Resilience**   
  Agile systems that take into consideration the technical robustness and compliance can help protect the system against bad actors

## Q. What are the components of AI Governance?

AI Governance can be measured as the following components:

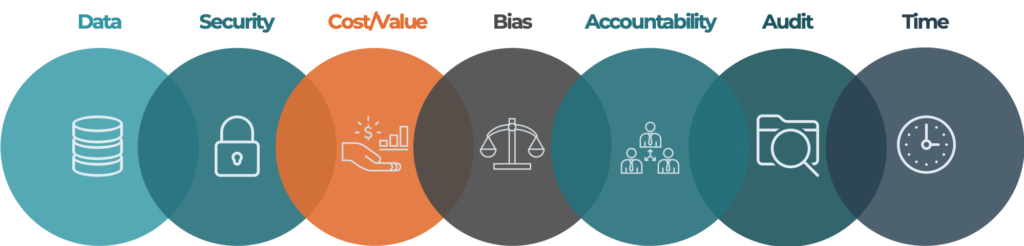


Figure 9: Components of AI Governance  
(Source: [2021.ai](https://2021.ai/))

* **Data**   
  Tracks the data flow from start to end to ensure that the data lineage and provenance is validated to ensure there are no loopholes
* **Security**   
  If someone in the AI System can manipulate the results of the model by tampering, this can lead to severe issues. This can be tacked in the future by using blockchain to imprint AI Systems
* **Cost and value of data**   
  Key performance indicators to track the cost of the data and the value obtained from the algorithm help measure effectiveness continuously
* **Bias**   
  Exposing selection and measurement bias with continuous automated tracking can help understand when a model drifts from its initial purpose (through self-learning). This should be monitored constantly to ensure the AI Ethics is maintained
* **Accountability**   
  Clarity on who are the individuals responsible for the system and accountable for its decisions is part of AI Governance of the future. All the way from security, loopholes, maintenance and monitoring
* **Audit**   
  Audit trails and third party reviews can ensure that systems that affect human life are held accountable
* **Time**   
  Model drift and impact overtime should be captured to ensure that the model is doing a more efficient implementation as compared to the traditional implementation

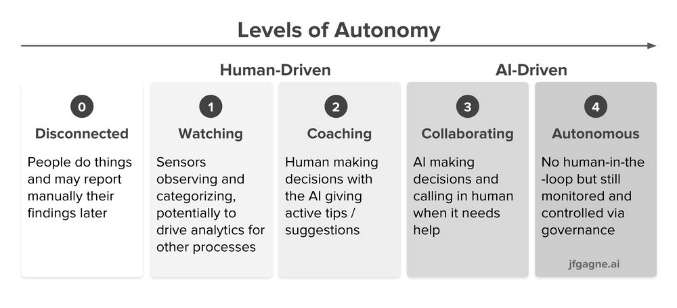


Figure 10: AI Governance Framework  
(Source: [aibotics](https://www.aibotics.tech/post/a-framework-for-ai-governance))

## Q. Good AI exists. Looking at the top companies in the world, we know that a robust framework exists where AI can scale. How do the best companies in the world build Scalable AI?

There are five principles using which we can Scale AI with AI Governance in place.

1. **Algorithms as micro-services**   
   Instead of making the entire AI workflow about the algorithm, consider algorithms as micro-services that can be subscribed to and managed independently. This leads to the following advantages that can be prescribed at Scale.
   * Reusability and lose coupling
   * Auto-scaling and scheduling
   * Portability and virtualisation
2. **Six Sigma, factory-like approach to manufacturing and managing algorithm**   
   Considering algorithms as part of the entire flow instead of the entire process means that we can focus more on the manufacturing of algorithms along with reducing errors. Monitoring KPIs and version control can help to manage multiple algorithms at Scale. This will also help to keep track of performance along with who worked on the algorithm last.
   * Standardised and automated workflows
   * Performance monitoring
   * Audit Trace
3. **Data Integration at Scale**   
   Most data architectures rely on a single source of truth. In real-world enterprises, companies rely on multiple sources of truth rather than trying to make a single route alone. Having multiple data integration routes helps optimise the operational as well as analytical use of data.
   * Experimentation in production
   * Big Data
   * Data Warehouse for core ETL tasks
   * Direct data pipelines
   * Tiered Data Lake
4. **Move from Batch to event-based triggers**   
   For larger streams of real-time data, batch processing is preferred as there is greater control over the end-to-end architectural needs. However, going ahead, it is advisable to move from Batch to event-based triggers as this will help reduce infrastructural costs with a just-in-time application.
5. **Leverage the cloud components to perform agile development**   
   To scale AI, we have to move past legacy infrastructure and leverage cloud components such as MLaaS, PaaS, SaaS and IaaS. This will give us access to the latest in security, technology, reduced cost and even world-class APIs.

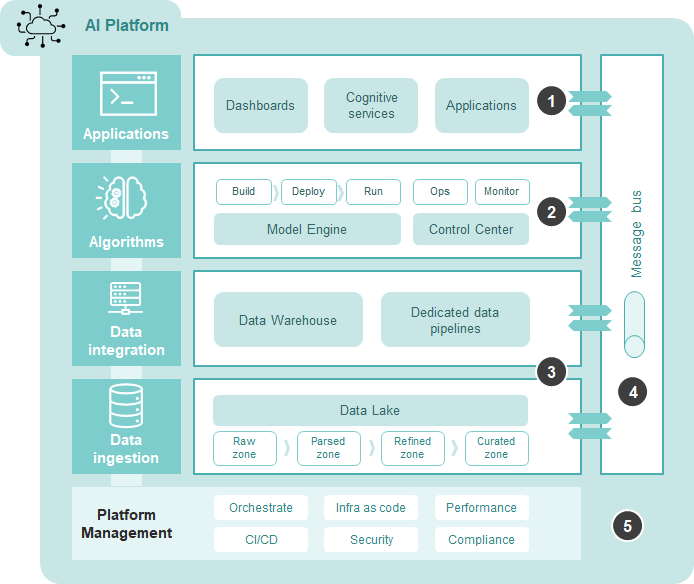


Figure 11: Scalable AI for Enterprises  
(Source: [TDS](https://towardsdatascience.com/how-leading-companies-scale-ai-4626189faed2))

## Q. What are the difficulties when it comes to scaling implementations of AI?

If leveraging and scaling AI was so easy, every company would have done it. It is difficult to Scale AI. Here are the top 5 difficulties that companies face when they attempt to Scale AI:

1. **Technical Performance**   
   When AI models are moved from development/testing to production, there are a whole set of new issues that become unstable. When AI is scaled, technical problems are imminent.
2. **Data Volumes and Veracity**   
   Data volume and quality decide how fast the AI System is ready to scale. The larger the set of predictions and usage, the larger is the implications of Data in the workflow
   1. Complex Technology Implications at Scale
   2. Onerous Data Cleansing & Preparation Tasks
3. **Business Processes & People**   
   People are the biggest surprise element in any AI Implementation. Companies want to be AI-first, but as they realise, AI is not just about training users but rather about amending processes, updating policies and putting in the right kind of business support.
   1. Internal, company-level changes
   2. Customer-facing changes
4. **Unexpected Behaviour**   
   When dealing with a machine with multiple moving parts and complexities, if the machine stops, it is extremely difficult to pinpoint exactly where the error has occurred. Similarly, testing AI implementations is not just about unit testing with the appropriate data, but rather designing for all use-cases to deal better when there are unexpected errors.
5. **Data Security and Governance**   
   These vulnerabilities can make or break AI Systems at Scale. As businesses grow to rely on an AI-first approach, complete transparency and control over the system are critical. One breach in Data Security can break the reputation of the stakeholder. AI Governance is the most critical component in this entire piece.

## Q. State out the Enterprise AI Journey.

Being mindful of where an organisation is in the AI journey can help make better decisions to ensure the company is headed in the expected direction. Following are some of the milestones that can help understand where the enterprise is at an organisational level:

* **BI and Apps**   
  Every company starts off with automation first. We need to understand and monitor the current state of data evolution at the enterprise level. This happens with the help of Business Intelligence Tools, analytics and reporting.   
  Tools: Power BI, Tableau, Qlik Sense
* **SaaS with AI**   
  Now, it is time to shoot for the low hanging fruit. Multiple hypotheses and use-cases are put forth that are attempted to solve with the Data Science. Enterprises in this stage shoot for immediately actionable insights.
* **AI Accelerators**   
  In this stage, companies are fully ready to leverage AI solutions. Solutions where speech, text and other structures, as well as unstructured data, can be used to make better decisions
* **Custom AI**   
  The final stage in the AI Journey is when a Custom AI solution to solve business problems can be made. It might be said that companies like Google are at this stage

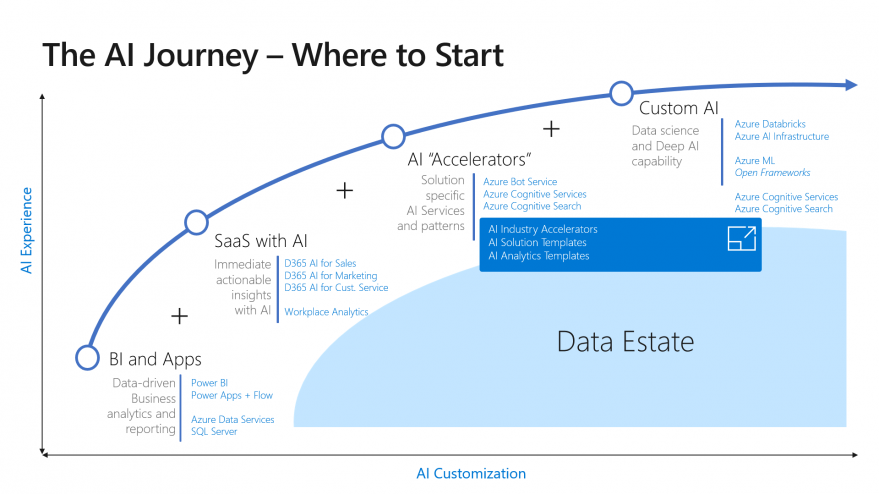


Figure 12: The AI Journey using Microsoft Azure  
([Source](https://blog.victoriaholt.co.uk/2019/01/the-ai-journey.html))

The figure showcases the steps and tools used in the journey using Microsoft Services. It is a plot of AI Customisation versus AI Experience.

# 6 XAI / Explainable AI

## Q. What are some of the common problems faced by companies when it comes to interpreting AI / ML?

There are multiple use-cases where companies have an in-house or hire an analytics vendor to perform analytics on a dataset and get the output. Even though there is a machine learning model in place along with the recommended solution, companies refuse to implement the proposed solutions in the business.

When AI / ML solutions are proposed, it is generally used to replace a heuristic (business-driven) model with a data-driven approach. However, the stakeholders view machine learning as a black box with an input and an output. Just showing them the output without a complete understanding of the model does not inspire as much confidence. Businesses tend to trust the model more if they understand the micro-decisions that lead to the final output.

For instance, SHAP and LIME are some of the popular approaches towards interpretable machine learning. Let's take an example of a problem where we are trying to predict if a customer is going to churn (1) or not churn (0).

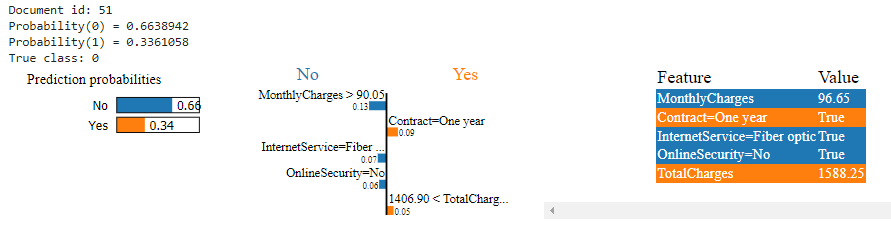


Figure 13: LIME Implementation to predict Customer Churn in the Telecom Industry  
(Source: [GitHub](https://github.com/anishmahapatra/Classification-Telecom-Customer-Churn/blob/main/Classification_Telecom_Customer_Churn_v5.ipynb) by [author](https://www.linkedin.com/in/anishmahapatra/))

Here is my implementation of LIME showcasing not just the result but also the reasoning behind the output that the customer will not churn. Below is the implementation using SHAP.

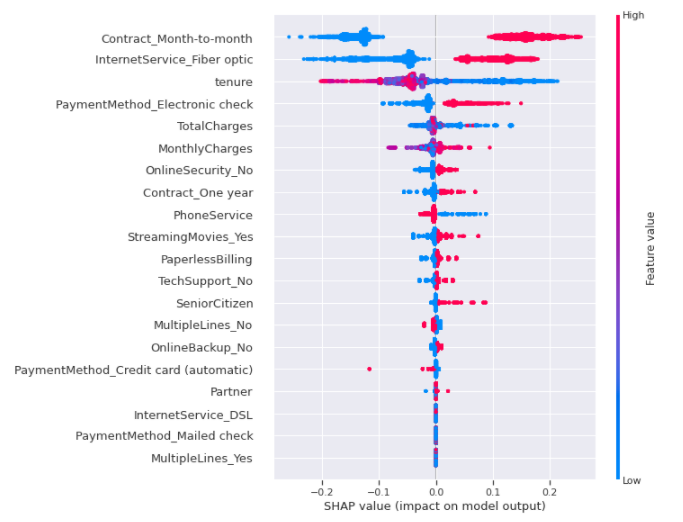
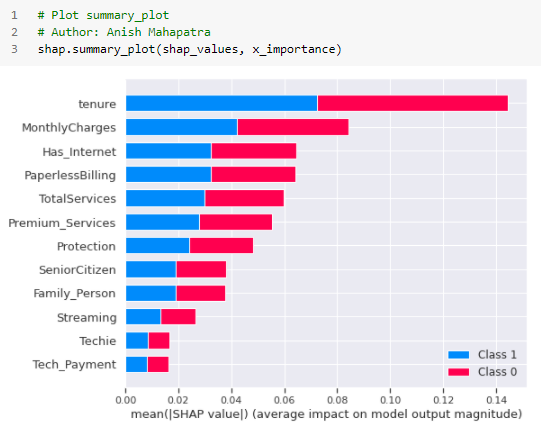
 

Figure 14: SHAP Implementation to predict Customer Churn in the Telecom Industry  
Source: ([GitHub](https://github.com/anishmahapatra/Classification-Telecom-Customer-Churn/blob/main/Classification_Telecom_Customer_Churn_v5.ipynb) by [author](https://www.linkedin.com/in/anishmahapatra/))

The diagrams above will help explain to the business the reasoning and the logic behind the decisions made in a model-agnostic approach.

## Q. Explain the concept of XAI and how it can be used in real-world implementations?

Explainable AI is the implementation of AI / ML models in such a manner that they can be understood by human experts. Simpler models are interpretable. More complex models are not very interpretable. As models move from a simple regression model to deep learning to solve problems in the pursuit to improve results, there is a new observation that can be made.

Never models have low interpretability and high predictability. The latest area of research is XAI or Explainable AI on how we can maintain the strides we have made in predictability while making interpretability better.



Figure 15: Black Box approach to machine learning

Following are some of the popular approaches in machine learning interpretability :

* **SHAP** takes a global view of machine learning models and uses Shapely values to leverage a global approach to interpreting results.
* **LIME** stands for Locally Interpretable Model-Agnostic Explanations. LIME focuses on local interpretability and can be used for all approaches (model-agnostic).
* **EBM** or Explainable Boosting Machines uses the GA2M framework, which leverages a generalised additive model with an interaction model added to it (this is still a relatively new framework)

## Q. AI/ML Models are black boxes that give us the desired output. What are some of the ways we can help the business feel comfortable with the models being implemented?

Some of the factors to bring explainability back to AI/ML Models are as follows:

* **Intention**: Understanding the reasoning behind a decision can help both identify ways to correct and improve the reasoning, thus leading to better results
* **Impact**: If the impact is a human's livelihood, the model is much more critical than a model that is trying to target the right demographic in a marketing campaign
* **Control**: Is the system allowed to make decisions autonomously, or does the system propose recommendations that are reviewed downstream by human operators before the final decision is made
* **Rate**: The number of decisions that the system makes and the audit and review mechanism
* **Rigour**: The system's robustness will reduce unpredictable behaviour for scenarios it has not been trained on, like unseen data or abnormal values
* **Law & Regulation**: The legal and regulatory framework that the system operates within, along with those accountable for the system's behaviour
* **Reputation**: The respect that people have for a system or organisation based on previous performance
* **Risk**: The classic question of risk versus reward. What are the outcomes of a wrong decision? Death or merely a few cents lost on the dollar.



Figure 16: Explainability is a balance between criticality and complexity  
([Source](https://lawtomated.com/))

All of these factors together combine to form better systems for Interpretable AI.

## Q. Explain some examples of tools and technologies that can help implement interpretable machine learning or XAI.

Some of the popular implementations of XAI are as follows:

* **SHAP**: It is a popular implementation that used **SH**apely **A**dditive ex**P**lainations (SHAP) to explain the output of any model globally. It is a model agnostic framework
* **LIME**: **L**ocally **I**nterpretable **M**odel-agnostic **E**xplanations is another popular model-agnostic framework that uses local interpretation to showcase the micro-decisions that the model makes before it comes up with the final output
* **Shapash**: This is an implementation that takes the visualisations from SHAP and LIME explanations and forms it as an easy-to-use web application. It is essentially a forked version of SHAP and LIME to make it easier to showcase it to business users
* **Explainer Dashboard**: Think of the best of SHAP and LIME. Now, add a lot more elements of machine learning interpretability / XAI and make a great web-based dashboard out of it for your use case. This is what the Explainer dashboard is
* **DALEX**: Dalex provides wrappers around ML frameworks. DALEX (mo**D**el **A**gnostic **L**anguage for **E**xploration and e**X**plaination. All of DALEX's plots are interactive as well
* **EBM**: Explainable Boosting Machines was created by InterpretML that leverages *glass-box* modules
* **ELI5**: This is an explainability package by MIT that provides local as well as global explanations

## Q. All of the conversations about XAI seem to be problems of the future. If you were to design an AI / ML model for a business now and productionalize a model, what are some of the considerations you would have as a leader of the project?

One of the common problems faced in the real world is that clients view the Data Science workflow as something that will yield results. Business teams try to show linear progress Sprint on Sprint to showcase that incremental work, however minimal, is being performed.

If Data Science were a linear activity, it would be called Data Engineering. Data Science Teams work in an extremely non-linear & complicated fashion but fail to educate the business about how Science is actually happening within the team. Rather than educating the business that Data Science is a set of experimental, non-linear attempts at obtaining something useful from the data, teams force-fit the results into the perception that the Data Science Team is moving towards the final goal.

As time passes and experiments are failing, the expectations of the business are on the rise. When they see the final result, there is a general disappointment as expectation generally does not match reality. In fact, I am so right about this that it surprises me.

*87% of Machine Learning models do not go into production.* – [*Venture Beat*](https://venturebeat.com/2019/07/19/why-do-87-of-data-science-projects-never-make-it-into-production/)

So, what are some of the ways that we can productionalize interpretable models for the business?

* **Be real and transparent with the business**: Instead of force-fitting results linearly, adopt a truly Agile approach to Data Science. Essentially, lay down the hypothes you are dealing with and Sprint by Sprint deal with each one and report back
* **Failures are good**: Don't be afraid to showcase failures to your stakeholders. This helps build trust and showcases that some experiments work and some don't.
* **Logging**: Make a dashboard early on in the project so that the business can keep track along with your team of the successful and failed attempts. This might help bring new perspectives to the table later on. Do not just showcase the highlights of the week once a week in a PowerPoint to the meeting. Leverage the dashboard to showcase the overall progress – do not be afraid to iterate!
* **Automate success**: For the experiments that work, make production-ready code and keep the blocks ready so that when the time comes, the team is set to implement along with the basic test cases
* **Be critical of the data**: One of the most common misses across some of the largest teams is that if we solve problem X in development, the ask becomes problem Y in production. Set up basic test cases for the data as well so that the system is robust!

# 7 Ethical AI / Federated Learning (TBD)

## Q. With a world being driven more towards a privacy-focus mentality, what are some of the recommended approaches companies/teams can take to?

Machine learning teams can work on actionable insights only if we are able to get access to data. When algorithms get so good that instagram and facebook ads alonst feel that they can hear you, people can get uncomfortable. Privacy

## Q. A common statement is "With the onset of the Digital Era". In the coming years, as AI started to take over more and more components of human life, the statement is going to transition to "With the onset of the AI era". Is Ethical AI a real concern or just hype? What are the ramifications?

A.

## Q. How can Ethical AI be implemented at an enterprise level? What are its implications for Enterprise AI use-cases and Governance?

Ethical AI is the practice of leveraging AI with good intention to empower employees and businesses. Ethical AI lets companies Scale AI with confidence. Right now, companies are in the development phase of what AI is going t be in the future. There is no single source of truth. Each company has their own Ethical AI Framework:

* [Google](https://www.blog.google/technology/ai/ai-principles/)
* [Microsoft](https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6)
* [Facebook](https://ai.facebook.com/blog/how-were-using-fairness-flow-to-help-build-ai-that-works-better-for-everyone/)

Ethical AI, also known as Responsible (or Trustworthy) AI, is the practice of using AI with good intention to empower employees and businesses, and fairly impact customers and society. Ethical AI enables companies to engender trust and scale AI with confidence.

## Q. With privacy focus coming to the forefront, a lot of attention has been brought to data collected. A new branch of data collection and processing for ai / ml is federated learning. Explain further.

A. [Federated Learning | Towards Data Science](https://towardsdatascience.com/understanding-federated-learning-99bc86a0d026)

## Q. Explain how a model can be monitored after it is moved to production. Break down the approach.

A. [MLOps: Model Monitoring 101 | Towards Data Science](https://towardsdatascience.com/mlops-model-monitoring-101-46de6a578e03)

# 8 Cyber Security AI

## Q. Cybersecurity is the need of the hour. What is a good way to classify all security-related tasks using the PPDR framework?

People perceive Cyber Security as a mere threat to the system of the data. It is easy to miss out on the fact that our world runs due to the transfer and exchange of data. As seen carefully, every single application in our life is merely an interface to a database. Think about it.

*Uber, BigBasket, Swiggy, PolicyBazaar, Paytm, Instagram, YouTube, GPay, Gmail, Amazon*

A security breach no longer means that we lose a few email ids and passwords. A security breach can be the difference between normal life and an alternate one. This was something that was showcased in the recent US Gas pipeline Cyberattack. ([Source](https://www.bbc.com/news/business-57112371)). A bunch of hackers arm-twisted the world's most powerful government body to pay them a ransom. Publicly. This would have been unthinkable a few years ago. On that interesting note, Gartner's PPDR Framework is one of the most recommended approaches to information security management systems for enterprise risk assessment.

* **Predict**   
  This is in the pre-attack phase. Periodic thread assessment and careful observation can help assess vulnerabilities. Bounty hunting programs are some of the more popular ways to do self-assess for threats.
  + Periodic Vulnerability assessment
  + Threat Hunting
  + Cyber Security Intelligence
* **Prevent**   
  Regularly being up to date with security patches and stress-testing systems can help prevent cyber attacks. Focusing on making cybersecurity process-driven and removing the human element can help.
  + Server Hardening
  + Security Patching
  + Source Code Review
* **Detect**   
  This is during the attack phase. Being able to detect that a cybersecurity attack is happening is critical to be able to cut losses and prevent further attacks. Robust systems set up can handle detection.
  + Perimeter Security Devices
  + Endpoint Security
  + Network Security
  + Web Application Security
* **Respond**   
  This is during the post-attack phase, where assessment and isolation of the portion of the network and devices need to be done. Incident reporting and logging can help to prevent further attacks in the future.
  + Identification of infected devices
  + Isolation of compromised devices
  + Incident response and reporting

## Q. How can machine learning be used within the space of Cyber Security. Broadly explain the various elements of Cyber Security.

On a broader scale, Machine learning can be used in Cyber Security for the following:

* Pattern analysis for CyberSecurity threats
* Anomaly Detection for application and network threats
* Automation of vulnerability checks
* Effective implementation can lead to saved costs

Following are a few cases of how machine learning is used in the field of Cyber Security:

* User entity behavioural analytics, deep learning, automation
* Assist IT professionals and defend against new cyberthreats
* Better predictive models, lower FPR, distil new metrics
* Fraud and anomaly detection
* Defend against new cyberthreats
* Better use of internal data and global repositories
* Tackle device influx and enhanced data loss prevention (DLP) solutions

## Q. Mention ten use-cases as to how AI / ML can be used within Cyber Security use-cases.

Instead of looking at machine learning and figuring out how to apply it to Cyber Security use cases, let's look at Cyber Security applications and see how Machine Learning can help.

* **Network Protection**   
  This refers to Intrusion Detection Systems (IDS), where machine learning can help using Network Traffic Analysis (NTA)
* **Endpoint Protection**   
  When we download an executable file and run it, the risk of malware is much higher than normal. Using machine learning to isolate and classify such risks can help secure systems
* **Application Security**   
  Machine Learning can help with Enterprise security or Web Application Firewalls (WAF) applications
* **User Behaviour**   
  User Behaviour began as Security Information and Event Management (SIEM). Gartner has a specialised framework to deal with User and Event Behaviour Analytics (UEBA)

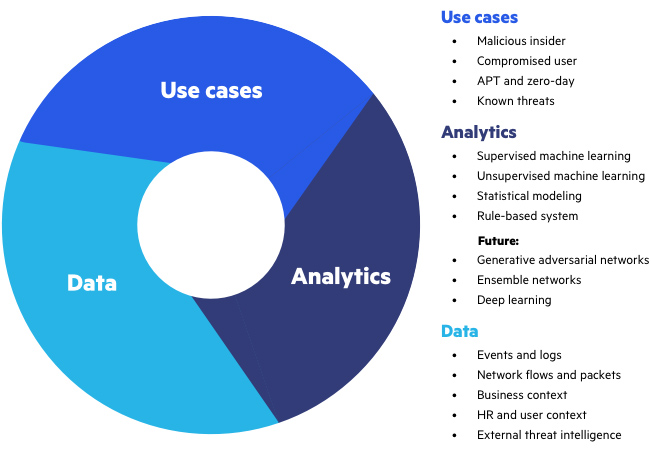


Figure 17: The three pillars of UEBA  
([Source](https://www.imperva.com/learn/data-security/ueba-user-and-entity-behavior-analytics/))

* **Process Behaviour**Security risks for use-case driven business risks. This is a customs problem and will depend on the domain, the horizontals and verticals of the business

## Q. Explain the flow of Cyber Security attacks and how AI / ML models can help plug the gaps.

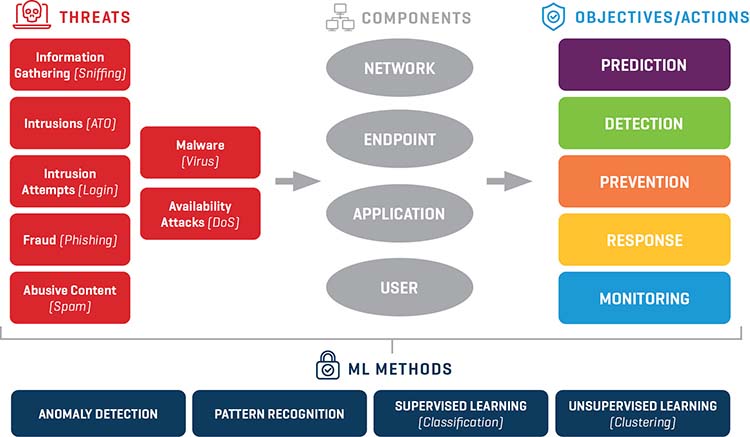


Figure 18: Cyber Security from a Machine earning perspective  
(Source: [Stout](https://www.stout.com/))

Cyber Security is critical at each part of the pipeline. There is no single part where Machine Learning can aid in keeping systems safe. At every step, there is scope for automation and machine learning to improve the quality of cybersecurity at a reduced cost. There are a few main reasons why Machine Learning Systems beat out more traditional approaches:

* Machine Learning can recognise abnormal patterns flag them easily. This can be set to as sensitive as required, depending on the use-case
* Machine Learning systems keep improving as they keep learning
* Since Machine Learning systems are automated, they require minimal intervention and are cost-efficient

## Q. How can Cyber Security be implemented across a PoC Team or at an enterprise level with the help of AI / ML?

Cybersecurity is a critical part of both small and large organisations. Following Information security practices that have been set up by enterprises is a good place to start. The three components that can be catered to in terms of cybersecurity at a broad level is people, process and technology.

* **People**   
  Companies do not realise the value of cuber security professionals until it is too late. Similar to a lot of other scenarios, prevention is better than cure.
  + Lack of skilled professionals
  + Data across defined boundaries
  + Social Engineering attacks
* **Process**   
  Business processes vary immensely even within the same enterprise. Catering to cybersecurity compliance along with balancing cost pressure can lead to better systems.
  + Cost pressure
  + Regulatory compliance
* **Technology**   
  This is the most expensive and critical element in the cybersecurity workflow. We can scale enterprise-wide and secure most applications with fundamental analysis on best practices org-wide.
  + Boundary-less enterprise
  + One-size fits all security technology
  + Speed of technology adoption

# 9 RPA: Robotic Process Automation

## Q. What is Robotic Process Automation? Explain in brief with a few examples.

As part of Gartner's Top Trends last year, number one is hyper-automation. RPA or Robotic Process Automation is a core automation technology that interacts with a digital system to take over tasks that are repetitive. It's great with rule-based systems that do the same thing over and over again. RPA is better with workflows that do not evolve or change. Think of RPA as support staff with less knowledge.

Examples of RPA include the following:

* Customer service automation (rule-based)
* Invoice Processing using OCR
* Automation of Sales Orders in the ERP as well as CRM Systems
* Payroll processing and automation
* Price comparison between vendors and manufacturers
* Processing HR Information
* Recruitment automation

Some of the benefits of RPA are accuracy, compliance, speed, reliability and increased productivity.

## Q. What is the difference between AI and RPA?

Technologies such as RPA can be considered as a subset of Artificial Intelligence. AI and RPA work hand in hand to automate complicated tasks that require more *thinking* along with *doing.*

In case you are still looking for it, there is no clear answer. It is like asking for the difference between your brain and your hand when you need to perform a task. The muscle memory from your hand works for a lot of repetitive use-cases, and when there is a change or anything new, your brain needs to come into play and decide on new processes.

Similarly, by combining RPA and AI, enterprises increase capabilities and make their processes more efficient.

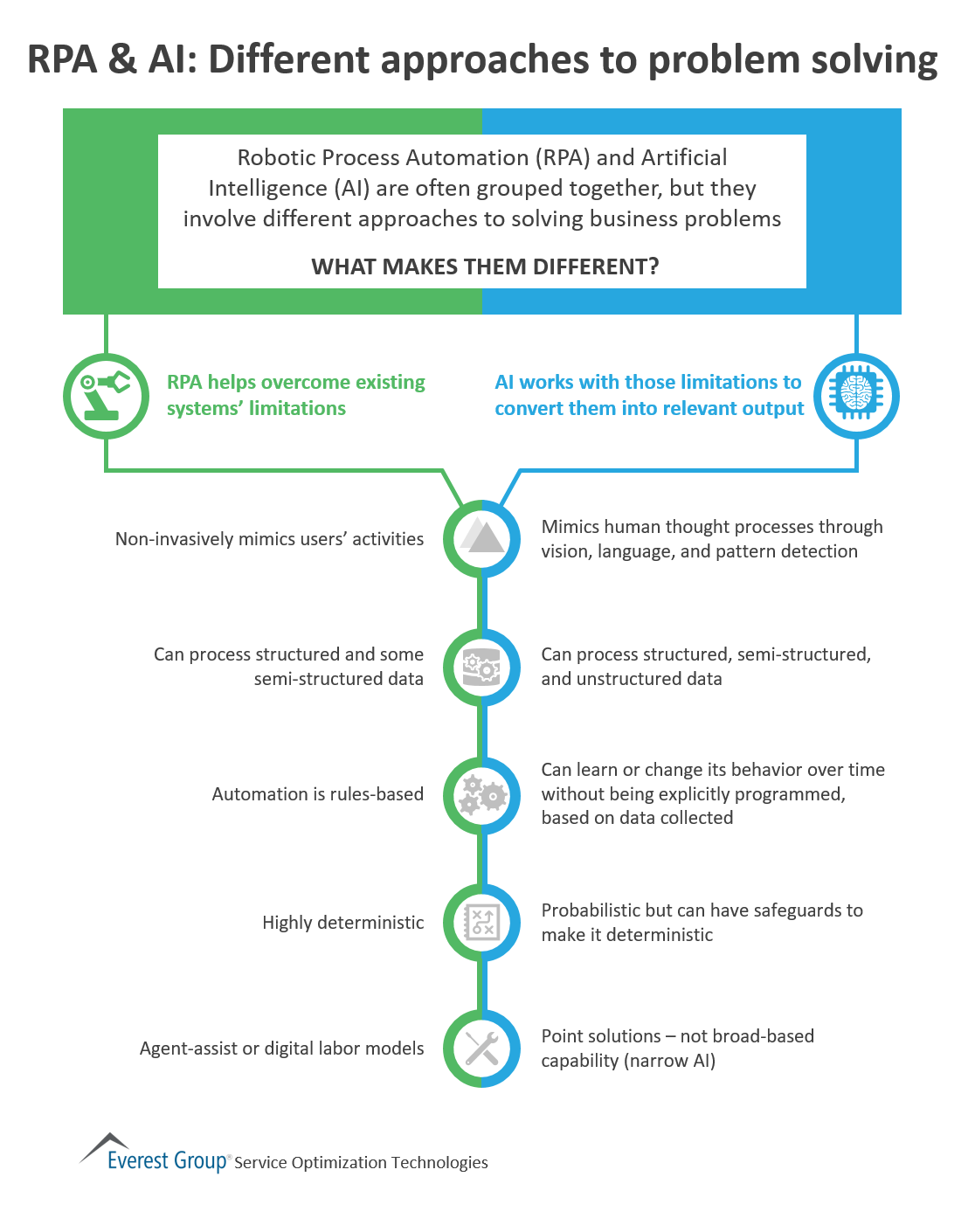


Figure 19: Differences between RPA and AI  
(Source: [Everest](https://www.everestgrp.com/))

Focusing on RPA helps you initially clearly define tasks, sub-tasks and focus on automation. Once the stakeholders are able to see the effectiveness of RPA at Scale, the eventual logical step is to pull in AI to perform more complicated tasks. AI and RPA implementation start out with a Proof of Concept (POC) that can later be scaled, depending on the use case. Some of the cases that can be deemed AI-worthy are:

* Workflows that have uncertain outcomes that require interpretation
* Highly variable processes that do not depend on a rule-based system entirely might evolve over time
* Processes that rely on unstructured data or AI Enhanced APIs

## Q. Explain the landscape of how RPA and AI can be used in tandem to increase revenue at an enterprise level? Discuss a few use cases.

Depending on where the enterprise is in its AI journey, there are different ways AI and RPA can be used to increase the bottom line. Just to recall, the following are a few examples of RPA:

* Moving files/folders
* Read/write to databases
* Scrape data
* Log into apps
* Extract structured data
* Fill forms
* Email events

Following are the use-cases with AI and RPA working in tandem:

* **Understanding Documents**: Rather than performing similar tasks, entity extraction and intent classification may also be performed
* **Classification of Emails**: Emails can be put into different buckets for further processing downstream
* **Semi-structured data**: Data such as images, text, speech and video data have nuances that will need to be analysed and understood on a case to case basis
* **Speech to text**: Speech data has multiple components that make it especially difficult to interpret
* **Chatbots**: Chatbots can help automate multiple elements of a workflow with the help of RPA and AI

## Q. What are the phases of RPA at an Enterprise Level?

* **RPA 1.0: Assisted RPA**
  + Objective: Improving worker productivity
  + Deployment: Worker's desktop
  + Limitations:
    - Partial automation
    - Difficult to Scale
* **RPA 2.0: Unassisted RPA**
  + Objective:
    - End-to-end automation
    - Scalable virtual workers
  + Deployment: Server (VMS)
  + Features:
    - Work orchestration (scheduling/queuing)
    - Centralised robot management
    - Robot performance analytics
  + Limitations:
    - Manual control and management of robots
    - Managing screen and system changes
* **RPA 3.0: Autonomous RPA**
  + Objective:
    - End-to-end automation
    - A scalable and flexible virtual workforce
  + Deployment: Cloud/SaaS (VMs)
  + Features:
    - Auto-scaling
    - Dynamic load balancing
    - Context-awareness
    - Advanced analytics and workflows
  + Limitations:
    - Processing unstructured data
* **RPA 4.0: Cognitive RPA**
  + Use of Artificial Intelligence (AI) technologies, including machine learning and Natural Language Processing (NLP), to enable:
    - Processing of unstructured data
    - Predictive and prescriptive analytics
    - Automation of tasks that involve judgment ([*Source*](https://www.everestgrp.com/))

## Q. Why are people doing RPA? Is it actually worth pursuing?

For people who are more familiar with automating processes, there might be less respect for RPA teams as it seems like there is not much getting done. Don't let Data Scientists ruin RPA efforts. RPA can save millions of dollars annually by automating simple tasks. To being with, that may be where the real savings for organisations may be.

[TCS, Infosys & Other IT Firms Can Fire 30 Lakh Employees Due To the Rise In Automation (Report)](https://trak.in/tags/business/2021/06/17/tcs-infosys-other-it-firms-can-fire-30-lakh-employees-due-to-rise-in-automation-report/)

This is due to Robotic Process Automation. Rather than trying to resist change, it is better to accept change and upskill yourself. Following are a few benefits of Robotic Process Automation:

* **Accuracy**: RPA bots do not make mistakes because they do not think; they just do
* **Low Technical Barrier**: There are no programming skills required to configure RPA bots
* **Compliance**: This is one of the main advantages of RPA. Compliance across various geographies can be adhered to perfectly
* **Non-Invasive Technology**: Systems do not need to be upgraded; no major initial investment as such is needed
* **Improved Employee Morale**: Everyone likes being valued. Automating rudimentary and repetitive tasks that add no value leaves the employee to find more engaging & interesting work
* **Productivity**: Process cycles are much faster as compared to the manual effort as bots don't take breaks or make mistakes
* **Reliability**: Processes can run 24/7 with no interruptions
* **Consistency**: Routine tasks are performed the exact same each and every time

# 10 GANs: Generative Adversarial Networks

## Q. What are GANs?

A. [Understanding Generative Adversarial Networks (GANs) | by Joseph Rocca | Towards Data Science](https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29)   
[A Gentle Introduction to Generative Adversarial Networks (GANs) (machinelearningmastery.com)](https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/)   
[Background: What is a Generative Model? (google.com)](https://developers.google.com/machine-learning/gan)

## Q. Provide an overall system view of GANs.

A. [Overview of GAN Structure  |  Generative Adversarial Networks (google.com)](https://developers.google.com/machine-learning/gan/gan_structure)

## Q. Explain some uses-cases on the variations of GANs.

A. [GAN Variations  |  Generative Adversarial Networks  |  Google Developers](https://developers.google.com/machine-learning/gan/applications)

## Q. Name some popular tools used for GANs.

A. [Top 10 Tools For Generative Adversarial Networks (GANs) (analyticsindiamag.com)](https://analyticsindiamag.com/top-10-tools-for-generative-adversarial-networks/)