ISSN No:-2456-2165

AWS Well- Architected Machine Learning- Best Practices to Achieve Business Goals

A White Paper

Ayesha Umaima
Data Engineer- Business Intelligence

Abstract:- Machine learning (ML) uses Algorithms to find patterns in data, learn from those patterns, and build mathematical models to make predictions about future data. Through improved disease detection, environmental protection, the transformation of products and services, and other factors, these Machine Learning solutions have the potential to transform lives.

This whitepaper gives you a list of tried-and-true best practises that are independent of technology and the cloud. When creating your ML workloads, you can use these guidelines and architectural principles, or you can employ them to make ongoing improvements after your workloads have gone into production.

I. INTRODUCTION

A wide range of global cloud-based products are available through Amazon Web Services, including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications. These products are on-demand, instantly accessible, and priced on a pay-per-use basis. More than 200 AWS services are offered, including data warehousing, deployment tools, directories, and content delivery. Without the initial set cost, new services can be provisioned fast. As a result, businesses, start-ups, small and medium-sized companies, and clients in the public sector have access to the building blocks they need to act fast in response to shifting business requirements.

The AWS Well-Architected Framework aids in your understanding of the advantages and disadvantages of the choices you make while developing cloud-based solutions. The six pillars of framework are the operation excellence, security, reliability, performance efficiency, cost optimization and sustainability. These architectural best practices help in operating and designing workloads in the cloud.

By responding to a set of questions for each pillar, you may evaluate your workloads against these best practices using the AWS Well-Architected Tool, which is free to use in the AWS Management Console.

- *Operational Excellence*: Includes the capacity to manage, operate, and analyse workloads. It makes it possible to generate corporate value and enhances supporting practises.
- *Security*: includes the capacity to safeguard data, systems, and resources. Through risk analyses and mitigation techniques, it enables the delivery of business value.
- *Reliability: includes a workload's capacity to recover fully from infrastructure or service outages. Ensures that a workload carries out its specified purpose accurately and consistently at the appropriate time.*
- *Performance Efficiency***:** Focuses on meeting requirements through the effective use of computing resources. It makes it possible to sustain effectiveness as demand shifts and technologies advance**.**
- *Cost Optimization:* includes the ongoing process of a system's enhancement and refinement during its entire lifecycle. It makes it possible to create and run cost-aware systems that reduce expenses, increase returns on investment, and produce desired business results.
- *Sustainability:* Raising effectiveness across all workload components by maximising the advantages from the given resources and lowering the overall resources needed.

For your ML models to produce correct results, the quality of the input data is crucial. Monitoring is necessary to continuously identify, fix, and minimize issues with accuracy and performance since data changes over time. You might even need to retrain your model using the most recent, refined data to do this. Workloads for applications rely on detailed instructions to resolve issues. Algorithms can learn from data using ML tasks in a continuous cycle of iteration.

II. WELL-ARCHITECTED MACHINE LEARNING LIFECYCLE

For each of the ML lifecycle phases, Well-Architected best practices are examined across the pillars of operational excellence, security, reliability, performance efficiency, and cost optimization. The 6 phases for the ML lifecycle referenced in this paper are illustrated in Figure 1 in a sequence.

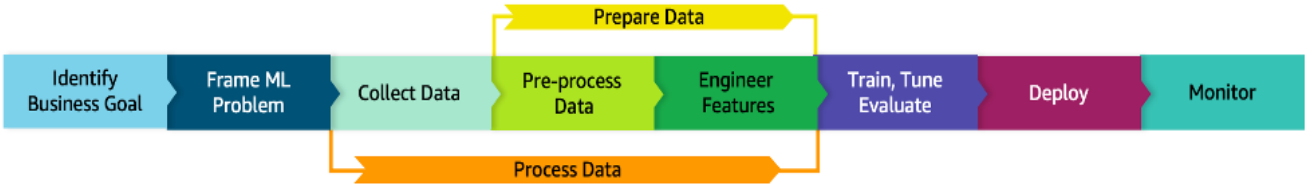

Fig 1 Machine Learning Life Cycle Process

III. IDENTIFY THE BUSINESS GOAL THROUGH MACHINE LEARNING LIFE CYCLE PHASE

The most crucial step is identifying the business goals. An organisation thinking about using ML should be clear about the issue that needs to be resolved and the potential benefits to the company. You must be able to evaluate business value in relation to certain business goals and success factors.

Make sure the algorithm has access to enough relevant, excellent training data for an ML-based strategy in order for it to succeed. Make sure the appropriate data sources are available and reachable by carefully evaluating the data.

This phase's actions are:

- Comprehend the needs of the business.
- Create a business inquiry.
- Examine the data needs and ML practicality of a project.
- Analyse the costs associated with data collection, training, inference, and inaccurate predictions.
- Decide on important performance indicators, such as allowable errors.
- Using the business question as a guide, define the machine learning task.
- Identify the essential features.
- Create concise, targeted POCs to validate the information above.
- Analyse whether adding outside data sources will enhance model performance.
- Identify production routes.
- Think about any new business procedures that may result from this implementation.
- Align the initiative with the appropriate stakeholders.

A. Operational Excellence

Plan to hire specialists with the awareness that extra training will be required as ML evolves, given the complexity and quick growth of ML technology. Maintain teams' skill levels, engagement, and motivation while constantly promoting accountability and empowerment.

B. Security

The AWS Cloud enables a shared responsibility model. While AWS manages security **of** the cloud, you are responsible for security **in** the cloud. This means that you retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data centre.

Model creation, model development, model training, and hosting are all handled by ML libraries and packages. Create a procedure to check all software and ML libraries required for the ML lifecycle's privacy and licence agreements. Make sure these agreements adhere to the security, privacy, and legal requirements of your company.

C. Reliability

Throughout the lifecycle, use the agreed level as a metric for evaluations and trade-off analyses. Understanding the reason for a prediction, performing audits, and adhering to regulations can all be made easier with explain ability. It can help establish trust by ensuring that the model is performing as predicted.

➢ *Recognize business needs*

- Trust is necessary for the use of AI systems in regulated domains.
- This can be developed by offering trustworthy justifications for the used predictions.
- Reliability, safety, and compliance standards may place a premium on model explain ability.

➢ *Choose a level of explain ability that is acceptable*

Share your thoughts on the project's level of explainability with all the project's stakeholders. Reach an understanding that enables you to fulfil business requirements.

D. Performance Efficiency

Key performance indicators (KPIs) pertinent to the business use case should be recorded using advice from business stakeholders. To determine acceptable model performance, the KPIs should be closely related to business value. Remember that uncertain machine learning inferences will not yield precise results. Establish the KPIs' minimum acceptable accuracy and maximum acceptable error. By doing so, it will be possible to manage the risk of fluctuating results while attaining the necessary business value.

➢ *Calculate the business's value of machine learning.*

Think about the following indicators of the business impact of automation and machine learning:

- How much will machine learning lower costs?
- How many additional users will be added by increased scale?
- How much more quickly will the company be able to react to changes like shifting demand or a disruption in supply?
- How many hours of manual work will be eliminated by machine learning automation?
- How much can machine learning alter user behaviour, such as churn reduction?

➢ *Review the tolerance for error and the hazards*

Calculate the business's impact of machine learning. To determine the key KPIs to optimise with machine learning, rank order the impact values. Set the cost of error for the automated inferences that the use case's ML models will make. Establish the business's tolerance for inaccuracy. As an illustration, figure out how inaccurate a cost reduction forecast would have to be in order to harm the business objective.

E. Cost Optimization

From the initial design of your very first proof of concept to the ongoing operation of production workloads, adopting the practices in this document can enable you to build and operate cost-aware systems that achieve business outcomes and minimize costs, thus allowing your business to maximize its return on investment

➢ *Define overall return on investment (ROI):*

- Estimate the cost of resources needed
- Develop a cost-benefit model and reassess as changes occur throughout the project.
- To quantify the costs of data and errors, evaluate and appraise the data pipeline, the ML model, and the anticipated quality of output conclusions.
- Specify the objectives of the ML project as research or development. A research project is intended to discover the value that could be achieved from an untested ML use case, and the returns will be long-term. A development project is intended for specific production improvements and is expected to deliver a faster return on investment.

➢ *Use managed services to reduce total cost of ownership (TCO)*

Minimize the possible future risks and failures through upfront understanding of the ML development process and its resource requirements. Adopt automation and optimization that can result in reduced cost and improved performance.

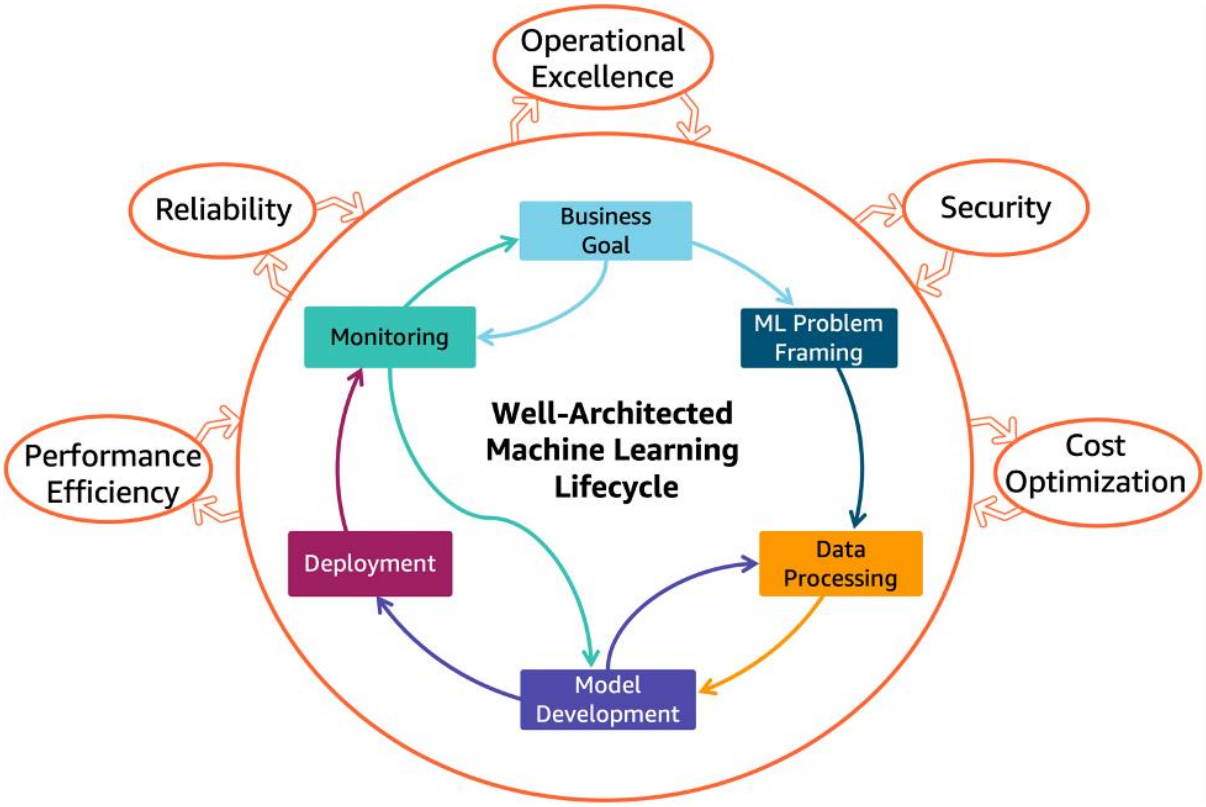

Fig 2: Well Architected Life Cycle

IV. CONCLUSION

Use these practices to help ensure that your ML workloads are architected with operational excellence, security, reliability, performance efficiency, and cost optimization in mind. When designing new workloads, think ahead and choose wisely. Make use of best practices to help you design and deploy new workloads more quickly. Utilize the guidelines to analyse current workloads frequently in order to spot, stop, and resolve possible problems before they become serious.

REFERENCES

[1]. AWS Well-Architected Framework
[2]. AWS Operational Excellence pillar
[3]. AWS Security pillar
[4]. AWS Reliability pillar
[5]. AWS Performance Efficiency pillar
[6]. AWS Cost Optimization pillar

ABOUT THE AUTHOR

Ayesha Umaima |Data Engineer Business Intelligence

A Master of Technology in Computer Science Engineering and with overall 11 yrs. of experience, Ayesha is on her journey of finding meaningful insights in data. Throughout her career, driven by a thirst for knowledge she has worn many hats: Business Analyst, Tableau Developer, Agile Advocate, Cloud Computing Enthusiast, and a Data Engineer. Her projects are mostly centred around Data Science and Machine Learning. Apart from instigating positive changes for clients, she has great affinity to reading and writing books. She enjoys travelling and is particularly fond of Snow Mountains.