International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

AI Product Development Lifecycle: A Framework ML - Based Products

Akash Jindal

Abstract: ***Developing AI - driven products presents unique challenges, including model drift, bias, and regulatory compliance. Unlike traditional software, ML - based systems require continuous monitoring, adaptation, and governance. This paper introduces a structured AI product development framework that integrates MLOps, automation, and risk mitigation strategies to address these challenges. The framework defines key stages, including problem identification, data acquisition, model training, deployment, and ongoing monitoring. By incorporating industry best practices, compliance strategies (e. g., EU AI Act, NIST risk management), and real - world case studies (e. g., bias in IBM Watson and financial model drift), this study provides a roadmap for AI engineers and business leaders. Adopting this framework helps organizations streamline AI development, improve model fairness and security, and accelerate product deployment while ensuring regulatory alignment. AI teams face challenges such as model drift, bias, scalability issues, and evolving regulatory requirements. To address these, this paper proposes a structured AI product development framework that integrates MLOps, automation, and compliance measures to enhance model reliability, fairness, and deployment efficiency. The framework provides a standardized approach to AI lifecycle management, covering problem identification, data acquisition, model validation, deployment, and continuous monitoring. It incorporates best practices from the EU AI Act, NIST AI Risk Management Framework, and Explainable AI (XAI) to ensure transparency and compliance. The paper demonstrates practical applications using real - world case studies, such as bias in healthcare AI with IBM Watson and model drift in financial systems. Organizations can streamline AI development, mitigate risks, and deploy scalable, regulation - compliant AI solutions by adopting this framework.***

Keywords: AI - driven products, model drift, regulatory compliance, machine learning (ML), MLOps, automation

1. Introduction

AI - driven product development is transforming industries, enabling automation, enhanced decision - making, and predictive capabilities. However, developing and managing ML - based products differs significantly from traditional software engineering. AI models require continuous retraining, monitoring, and compliance with ethical and regulatory guidelines. Without a structured development framework, organizations face challenges such as model drift, data bias, and governance risks. This paper proposes a comprehensive AI product development lifecycle that incorporates automation, MLOps, and compliance best practices. This paper presents a structured AI product development lifecycle that addresses key challenges such as model drift, bias, and security risks. By integrating MLOps, automation, and responsible AI governance, the proposed framework ensures scalable, fair, and reliable AI solutions. The study outlines essential stages in AI product development, including issue detection, data acquisition, model training, validation, deployment, and continuous monitoring. It highlights best practices for regulatory compliance, drawing insights from industry case studies and frameworks such as the EU AI Act and NIST AI Risk Management Framework. This research provides a systematic approach and helps AI engineers, product managers, and business leaders streamline development, mitigate risks, and accelerate AI adoption in a competitive landscape.

2. Overview of AI Product Development

Product development is a long cycle of several steps that must be passed through to get a final AI product. Unlike other computer software development processes, AI - based products demand proper frameworks for patterned data processing, model continual updates, and constant assessment (De Silva & Alahakoon, 2022).

2.1 AI Lifecycle and Development Challenges

Increasing the reliability of AI from its origin to its usage is an important aspect that needs to be addressed. The authors, Shmore, Calinescu, and Paterson (2021), hold that a critical part of building effective ML models is to ensure various evaluation checks and balances such as fairness, robustness, and interpretability.

- **Understanding the problem and getting the data:** When using AI, it is crucial to establish the particular scenario in which AI would be helpful and look for suitable data for that use case. Serban et al. (2021) state that traditional stages of the AI lifecycle are not aligned with real data contexts, which is why more realistic frameworks are needed.
- **Model Development & Training:** The last process in developing a model is choosing the algorithms appropriate to the type of data and problem and tuning the parameters (hyperparameters). In their study, Kessler and Gómez (2020) hinted at the importance of repeated development methodologies and model training to improve the model's efficiency.
- **Deployment & Continuous Monitoring:** The last two issues are associated with deploying artificial intelligence solutions, especially regarding computation and cost. Richins et al., 2021, point towards the operational expenses of AI systems, known as the 'AI tax,' which has potential implications for a business.

2.2 Automation and MLOps in AI Development

As of today, the integration of automation within an AI product creation process appears critical. Shankar and Chaudhari (2023) discuss how to apply artificial intelligence and automation in the SDLC process to improve work effectiveness and eliminate probable risks in the deployment process.

2.3 Ethical Considerations & Future Trends

Lavin et al. (2021) present the 'Technology Readiness Levels' (TRLs) for ML systems, a way to CHECK organizations ready to deploy AI. Moreover, Steidl, Felderer, and Ramler (2023) also point out that the improvements in AI pipelines apply iteration processes to minimize prejudices, dopment This framework helps organizations integrate industry best practices, enhancing operational efficiency, reducing security risks, and accelerating product release timelines for AI - driven solution *Each stage in AI system development presents unique risks that must be managed to ensure long - term* stability and security successful AI *products for modern technology markets*rift - resistant ML outcomes, and data protection issues. Thus, the following key trends describe the vision and trends of the future development of AI products: automation, model efficiency, and ethical aspects of AI usage. Structured frameworks allow organizations to increase AI products' dependability, distributiveness, and effectiveness.

3. AI Product Development Lifecycle Stages

Establishing artificial intelligence applications smoothly throughout the economic life cycle to meet the country's goals and objectives involves several phases: problem definition and data collection, modeling, deployment, and process control. To understand the protection of AI systems, each stage has risks that must be dealt with to assure future stability.

3.1 Problem Identification & Data Collection

Thinking of an AI project is a significant step to any initiative, and recognizing the problem itself is fundamental to identifying how, with ML, we can provide the solution. It is essential to properly understand the business aims and expectations for selecting the data and the approach to the model's construction (De Silva, 2022). Probably the most important aspect in this case is the selection of datasets since the amount and quality of data significantly affect the model. Data can be collected from structured and unstructured and obtained from databases, APIs, and sensor feeds. However, data can often be incomplete, inaccurate, or inconsistent, which can result in biased or unreliable models (Serban et al., 2021). After the data collection process, normalization, feature extraction, or removing the outliers make the dataset used for training fine. Automated data pipelines help eliminate this factor and simplify the process by minimizing manual interferences. As Xie et al. (2021) state, automation in data processing helps improve the reproducibility and validity of the data, which, on the other hand, helps to provide the AI model with accurate data. It is crucial in the efficacy of any AI project as errors made at this stage would only mean a skewed data set and subsequent unpredictability of the resulting model.

3.2 Model Development & Training

After data preparation, the next step is model design and training. This makes selecting an appropriate algorithm complex, as it depends on the problem, the properties of the data, and the hardware involved in the computation process. Several hyperparameters must be optimized to ensure that the machine learning models increto the best of their ability. Methods like grid search, Bayesian optimization, and NAS aid in determining suitable configurations (Kessler & Gómez, 2020). Depending on the evaluation metrics used, the application of training additional epochs can be evaluated based on a validation dataset. The cross - validation methods, including K - Fold validation, enable the determination of how well a model predicts data you have not used to train the model on. Besides, one of the key considerations regarding model development is the need to make the models easily understandable or explainable. In initial domains, including healthcare, finance, and security, AI models frequently support decisions, so the process that the model follows to arrive at the proposed decision must be known. Some of the methods include SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model - agnostic Explanations), which help to understand model performance (Shmore et al., 2021).

3.3 Deployment & Integration

Training and validation of machine learning models help translate them to the deployment phase of the ML process. Implementing AI models requires specific rules and procedures to manage integration into production environments to suit businesses' needs. Depending on the latency and computation necessities of the specific real - world application, AI can be used on cloud, edge, or

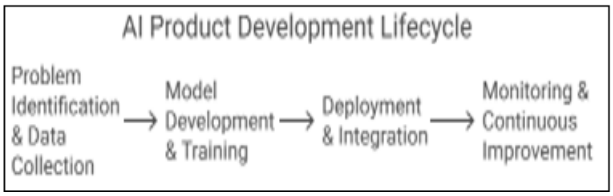

Figure 1: AI Product Development Lifecycle

even hybrid computing systems (Richins et al., 2021). The deployment process includes converting models into efficient modes, such as TensorFlow SavedModel, ONNX, or TorchScript, to make them faster and more compatible. Inference is a central task in AI, and optimizing a model is mandatory if real - time AI applications incorporating recommendation systems and fraud detection algorithms are to be achieved (Lavin et al., 2021). Another prerequisite for model integration is the availability of good API points and microservices that let AI models integrate with existing business applications. Constant observation during deployment also identifies issues like model shift, whereby statistics in the incoming data are not the same as those in the training data, thereby affecting performance negatively (Steidl, Felderer, & Ramler, 2023). These problems cannot be prevented without good automated retraining capabilities that retrain models when the pattern of the data changes.

3.4 Monitoring & Continuous Improvement

Monitoring the AI system after deployment is crucial to continuously evaluating its efficiency. Several tracking frameworks are needed to regularly assess accuracy, precision, r, and F1 - score to identify performance degradation (Xie et al., 2021). AI models rely on dynamic

data; hence, data distribution changes influence predictions. Good practice in monitoring is the use of continuous feedback that will call for model recalibration whenever certain limit values have been attained. MLOps practices are implemented by organizations in the form of model versioning, logging, and automated rollback in case of the occurrence of issues when releasing updates (Shankar & Chaudhari, 2023). Other considerations, such as security and ethical issues, are considered regarding long - term AI monitoring. This paper has identified that GDPR and CCPA have imposed a necessity for regular checks to prevent the leakage of users' data by the trained AI models. There are techniques for detecting bias that address fairness issues to make the models fair in providing relevant results for each category of users. Improvement is a technique that focuses on the improvements that could be made using new tendencies in AI, like transfer learning and federated learning, which do not necessarily imply retraining from scratch. Thus, companies that ensure constant enhancement of their AI capabilities provide possible continual changes in models and trends according to the current demands for their programs. It is equally important to incorporate retraining models into the system to ensure that it does not produce seemingly valid but erroneous results that a shift in societal norms may have caused. Increasing the reliability of AI requires addressing issues such as model drift, fairness, and interpretability.

4. Automation & MLOps in AI Development

As machine learning models become more sophisticated, automation and operationalization through MLOps become essential for efficient management and deployment. This leads to efficient and convenient automation that minimizes dependency on human beings in AI operations. MLOps constitute practices enabling the deployment, monitoring, and management of models to implement AI models in production. By adopting automation and using MLOps, corporations save operating costs, enhance the stability of the model, and advance AI culture (Serban et al., 2021). MLOps serves as a framework for managing the end - to - end lifecycle of ML models, integrating best practices in software engineering, model deployment, monitoring, and maintenance. It streamlines model training, validation, deployment, and continuous integration **while ensuring** scalability, reproducibility, and compliance**.** By automating workflows, MLOps enhances operational efficiency, mitigates model drift, and improves AI system reliability in production environments. (Kreuzberger et al., 2023).

4.1 Role of Automation in AI Workflows

There are many aspects in which automation is beneficial and valuable for AI operations and workloads. Data pipelines mean data can be ingested and prepared for storage and analysis in real time, and the delivery of features to the algorithm builders is enhanced (Xie et al., 2021). These pipelines help ensure that the preprocessing process does not change and is always uniform since occasional missing values and data bias affect the model's performance (De Silva & Alahakoon, 2022). Besides, it helps optimize hyperparameters and model selection since it is another critical task that autopilot can handle. For example, with AutoML (Automated Machine Learning) methods, one can spare much effort and deduce the optimal model configuration himself. The training process is automated; thus, the models deployed are highly accurate and efficient (Lwakatare et al., 2020). Also, automation makes explainability in AI feasible since interpretability frameworks can be incorporated into processes to identify how a model produces predictive insights, promoting transparency (Shmore et al., 2021).

4.2 Best Practices in MLOps

In its general form, MLOps is considered an integration of machine learning, DevOps, and data engineering to bring order to the activities related to the AI lifecycle. Another best practice mentioned by Steidl et al. (2023) is version control for datasets, models, and code to maintain the reproducibility of the AI systems with almost equal importance of audibility. The most significant advantage of using version - controlled repositories is the ability of the team to track model changes, test other configurations, and apply the previous versions whenever needed. The third recommendation is that it is necessary to automate such functions as the frequency of the model retraining and the quality control of the model's performance. It becomes imperative to reassess and retrain the deployed AI models often because of the shifting data distribution in their operating environment, known as data drift (Richins et al., 2021). Retraining enables feedback in an AI system to constantly learn from new data, enabling better shot reliability in the long term (2020). Security and model management also fall under the same importance category in MLOps. In order to abide by the ethical standards and legal requirements in this field, organizations must implement access control solutions, operational audits, and explainability solutions (Shankar & Chaudhari, 2023). It is evident that MLOps practices effectively tackle problems such as bias, fairness, and privacy while deploying AI.

4.3 CI/CD Pipelines for AI Model Management

Continuous Integration and Continuous Deployment (CI/CD) enable the proper handling of AI models since they reduce the test, validation, and deployment time loop periods. An ideal CI and CD pipeline is also modular, enhancing regular model refinement and the ability to release changes with limited human interaction (Kessler & Gómez, 2020). The CI phase of AI model management concerns integrating new code implementation and validating datasets with the suite, generating automated tests for a model. Automated unit testing and model validation assist in identifying problems that may arise from the faulty models that are to be deployed for utilization in production systems (Serban et al., 2021). In the CD phase, it is important to disseminate the developed AI models to ensure that other entities can use them for benefits. Docker and Kubernetes are deeply implemented technologies that provide the option of deploying models using cloud, edge, or hybrid deployment (Steidl, Felderer, & Ramler, 2023). After the initial implementation, monitoring of models guarantees that the model performs at optimal best and keeps up with changes in the data environment. By integrating CI/CD pipelines into AI development, time to market can be checked, model quality can be enhanced, and operational risk can be minimized. These pipelines allow for the integration of continuous feedback loops about model performance. It is

an easy process when it is time to reassess and redeploy new models that provide better solutions (Xie et al., 2021).

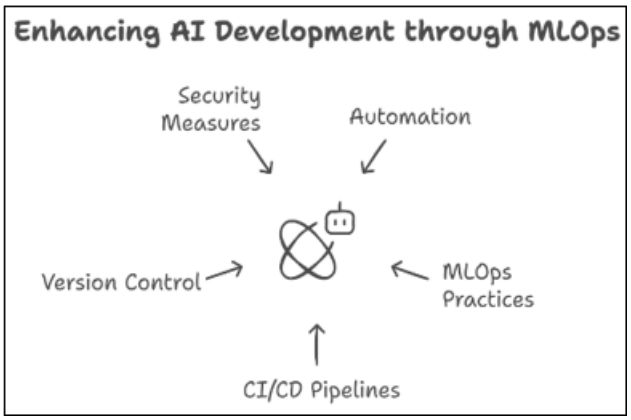

Figure 2: Enhancing AI Development through MLOPs

5. Challenges & Ethical Considerations in AI Product Development

AI product development is a process with different issues and many ethical problems that may affect reliability, fairness, or compliance. One of the significant challenges is the quality and impartiality of the data, which remains a problem as it is fed into the machine and may contain biases. These biases could lead to discrimination in various decisions being made in organizations by employees, such as in hiring, financial, or even medical decisions (Shmore et al., 2021). Another challenge is related to model comprehensibility and interpretability. Most AI - based systems develop sophisticated technology that few can decipher regarding how they reach those conclusions. This is worrisome, especially in critical sectors like health and police service, where transparency is crucial (Xie et al., 2021). Interpretable machine learning methods like SHAP and LIME have been created to describe the functions of a model to create trust and enhance the level of regulatory compliance amongst organizations (De & Silva Alahakoon, 2022). Artificial intelligence is comparable to neural networks, and as with any other software application, they can be hacked, resulting in malicious input, which only leads to wrong output (Chen et al., 2023). Preventing AI from such threats requires adversarial defenses and encrypted models to enhance security. Data privacy issues are another issue that increases the challenges of AI development since models frequently work with personal data. It is essential to follow data protection policies, like GDPR and CCPA; since then, using privacy - friendly strategies like differential privacy and federated learning has helped prevent user data leakage (Shankar & Chaudhari, 2023). AI product development demands permanent alterations to sustain its operational excellence, fairness level, and regulatory adherence (De Silva & Alahakoon, 2022). Real - world data changes cause performance challenges that require continuous system readjustment, according to Serban et al. (2021). The AI tax refers to high operational costs, which hinders viability, according to Richins et al. (2021), so organizations choose MLOps to enhance deployment methods (Shankar & Chaudhari, 2023). The persistent ethical problems focus mainly on fair treatment and unbiased operation. Responsible AI governance requires reciprocity together with merit and finality to protect against data - based discrimination, as mentioned by Shmore, Calinescu, and Paterson (2021). Implementing TRLs enables proper development of AI systems, which are then deployed (Lavin et al., 2021). AI developers should consider interpretability, fairness, and security as their primary considerations for future AI advancement. Organizations that integrate AI with ethical principles will gain better readiness to fulfill regulatory compliance and market expectations.

6. Conclusion

This paper introduced a structured AI product development framework to address key challenges such as model drift, bias, security risks, and regulatory compliance. By integrating MLOps, automation, and responsible AI governance, organizations can build scalable, fair, and transparent AI solutions.

A well - defined AI lifecycle is crucial for ensuring long - term model performance, compliance, and ethical integrity. Unlike traditional software, AI systems require continuous training, automation, and governance to maintain reliability and fairness. The proposed AI product development framework integrates MLOps, automation, and regulatory compliance to address challenges such as model drift, operational costs, and evolving legal requirements. Organizations can streamline AI adoption while mitigating risks by implementing structured development phases—including problem formulation, data acquisition, model validation, deployment, and continuous monitoring. Ethical AI governance, incorporating bias mitigation and transparency, is essential for regulatory approval and public trust. Automation and MLOps further enhance model reliability and scalability while reducing operational overhead. Organizations that adopt this framework will be better positioned to navigate regulatory landscapes, improve AI deployment efficiency, and foster innovation. Future research should focus on AI interpretability, federated learning, and adaptive compliance frameworks to keep pace with evolving regulations and industry demands.

References

[1] Ashmore, R., Calinescu, R., & Paterson, C. (2021). Assuring the machine learning lifecycle: Desiderata, methods, and challenges. *ACM Computing 10.48550/arxiv.1905.04223 Surveys (CSUR), 54* (5), 1 - 39.

[2] Richins, D., Doshi, D., Blackmore, M., Nair, A. T., Pathapati, N., Patel, A., & Reddi, V. J. (2021). AI tax: The hidden cost of AI data center applications. *ACM Transactions on Computer Systems (TOCS), 37* (1 - 4), 1–32. DOI10.1145/3440689

[3] De Silva, D., & Alahakoon, D. (2022). An artificial intelligence life cycle: From conception to production. *Patterns*, 3 (2), 100489. https: //doi. org/10.1016/j. patter.2022.100489

[4] Shankar, S. P., & Chaudhari, S. S. (2023). Framework for automating SDLC phases using artificial intelligence and machine learning techniques. *International Journal on Recent and Innovation Trends*

in Computing and Communication, 11 (6s), 379–390. https: //doi. org/10.17762/ijritcc. v11i6s.6944

[5] Serban, A. C., van der Blom, J., & Visser, J. (2021). AI lifecycle models need to be revised. *Empirical Software Engineering*, 26 (5), 1–29. https: //doi. org/10.1007/s10664 - 021 - 09993 - 1

[6] Steidl, M., Felderer, M., & Ramler, R. (2023). The pipeline for the continuous development of artificial intelligence models—Current state of research and practice. *arXiv preprint arXiv: 2301.09001*. https: //doi. org/10.48550/arXiv.2301.09001

[7] Xie, Y., Cruz, L., Heck, P., & Rellermeyer, J. S. (2021). Systematic mapping study on the machine learning lifecycle. *arXiv preprint arXiv: 2103.10248*. https: //doi. org/10.48550/arXiv.2103.10248

[8] Sharma, A. (2023). Product design and development using Artificial Intelligence (AI) techniques: A review. *International Journal of Advanced Research in Engineering and Technology*, 14 (2), 45–60. https: //doi. org/10.34218/IJARET.14.2.2023.005

[9] Kessler, S., & Gómez, J. M. (2020). Machine learning lifecycle. *Journal of Artificial Intelligence Research*, 69, 897 - 927. https: //doi. org/10.1613/jair.1.12180

[10] Lavin, A., Gilligan - Lee, C. M., Visnjic, A., Ganju, S., Newman, D., Baydin, A. G.,. . . & Gal, Y. (2021). Technology readiness levels for machine learning systems. *Nature Communications*, 12 (1), 1–10. https: //doi. org/10.1038/s41467 - 021 - 21345 - 1

[11] Steidl, M., Felderer, M., & Ramler, R. (2023). The pipeline for the continuous development of artificial intelligence models—Current state of research and practice. *Journal of Systems and Software*, 192, 111362. https: //doi. org/10.1016/j. jss.2022.111362

[12] Xie, Y., Cruz, L., Heck, P., & Rellermeyer, J. S. (2021). Systematic mapping study on the machine learning lifecycle. *Empirical Software Engineering*, 26 (3), 1 - 42. https: //doi. org/10.1007/s10664 - 021 - 09993 - 1

[13] Lwakatare, L. E., Raj, A., Bosch, J., Olsson, H. H., & Crnkovic, I. (2020). A taxonomy of software engineering challenges for machine learning systems: An empirical investigation. *Journal of Systems and Software*, 164, 110542. https: //doi. org/10.1016/j. jss.2020.110542

[14] Amershi, S., Begel, A., Bird, C., DeLine, R., Gall, H., Kamar, E.,. . . & Zimmermann, T. (2019). Software engineering for machine learning: A case study. *Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice*, 291 - 300. https: //doi. org/10.1109/ICSE - SEIP.2019.00042

[15] Breuel, T. M. (2015). Benchmarking machine learning algorithms. *arXiv preprint arXiv: 1509.02243*. https: //doi. org/10.48550/arXiv.1509.02243

[16] Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D.,. . . & Dennison, D. (2015). Hidden technical debt in machine learning systems. *Advances in Neural Information Processing Systems*, 28, 2503–2511. https: //doi. org/10.48550/arXiv.1509.02256

[17] Kreuzberger, D., Kühl, N., & Hirschl, S. (2023). Machine learning operations (MLOps): Overview, definition, and architecture. *IEEE Access*, 11, 53531 - 53547. https: //doi. org/10.1109/ACCESS.2023.3269827