

**Fig.1 Production Deployment ML System Architecture.**

**Production Deployment Questions - Based on ML System Architecture**

**Question 1: Assuming the business likes your model, what are the next steps to go from the Jupyter Notebook you've created to a productionised service? Do you have experience with doing this previously?**

**Answer:**

**Based on our architecture diagram, the transition involves several key stages:**

**Data Processing Layer (Apache Airflow):**

* Convert notebook data processing into scheduled Airflow DAGs.
* Implement data validation using Great Expectations for incoming Excel files.
* Set up automated ETL pipeline to PostgreSQL feature store.
* Create data quality monitoring and alerting systems.

**ML Pipeline Integration (MLflow):**

* Refactor model training code into production-ready Python modules using Object-Oriented Programming (OOP).
* Create modular classes for data preprocessing, feature engineering, model training, and prediction.
* Implement inheritance and polymorphism for different model types and preprocessing strategies.
* Set up MLflow tracking server for experiment management and model registry
* Implement automated model validation framework.
* Create model versioning and rollback capabilities.

**API Development (FastAPI):**

* Build REST API endpoints for real-time claim probability predictions using modular OOP design.
* Create service classes for prediction logic, data validation, and response formatting.
* Implement design patterns (Factory, Strategy) for scalable code architecture.
* Add authentication and authorization for secure access.
* Create comprehensive error handling and logging.
* Implement unit testing for individual API functions and model components.
* Develop integration testing to validate end-to-end data flow from Excel to predictions.

**Cloud Deployment:**

* Containerize application using Docker for consistent environments.
* Deploy to cloud platforms: AWS EC2/Elastic Beanstalk or Azure Web Apps.
* Set up CI/CD pipeline using GitHub Actions for automated deployments.
* Implement auto-scaling and load balancing for production traffic.

**Frontend Development (Streamlit):**

* Create business dashboard for underwriters and managers.
* Build prediction interface showing individual customer risk scores.
* Develop monitoring dashboard for model performance and business KPIs.
* Implement reporting tools for regulatory compliance.

I do have hands-on experience deploying ML models in production environments. I do understand the technical architecture and would collaborate closely with MLOps engineers, DevOps teams, and cloud specialists to ensure proper implementation following industry best practices and established frameworks.

**Question 2: What considerations are there for ensuring that if you productionised this model, the business could leverage it?**

**Answer:**

**1.Technical Integration Requirements:**

* Real-time API response (sub-second) for underwriting workflow integration.
* Scalable infrastructure to handle peak application volumes during busy seasons.
* High availability with 99.9% uptime to support critical business operations.

**2.Business Process Integration:**

* Seamless workflow integration with existing underwriting systems and databases.
* User-friendly Streamlit interfaces that don't disrupt current underwriter workflows.
* Flexible threshold management allowing business users to adjust claim probability thresholds.

**3.Performance and Monitoring:**

* Real-time monitoring of model accuracy and prediction quality using MLflow.
* Business KPI tracking showing actual vs predicted claim rates.
* Data drift detection to identify when model retraining is needed.
* Automated alerting when performance degrades below acceptable thresholds.

**4.Governance and Compliance:**

* Model explainability tools for individual prediction explanations.
* Version control for all model changes with rollback capabilities.
* Bias monitoring to ensure fair treatment across customer segments.

**Question 3: What are the steps you would take to provide this to the business? What assumptions are you making for this to be possible?**

**Answer:**

**1. Infrastructure Setup and Validation:**

* Deploy ETL pipeline using Apache Airflow for automated data processing.
* Set up PostgreSQL database with proper security and backup procedures.
* Configure MLflow server for model registry and experiment tracking.
* Validate data quality and model performance on historical data.
* Set up monitoring infrastructure with alerting capabilities.

**2**. **API Development and Testing:**

* Build FastAPI service with comprehensive error handling and logging using OOP principles.
* Create modular class structure for API endpoints, business logic, and data processing.
* Implement unit tests for model functions, data processing, and API endpoints.
* Create integration tests for full pipeline validation (Excel → PostgreSQL → ML → API).
* Deploy to staging environment on AWS/Azure for testing.
* Create Streamlit dashboard for business user interaction.

**3. Stakeholder Education and Handover:**

* Conduct training sessions for underwriters on model interpretation and usage.
* Deliver technical presentations to business stakeholders, and management teams.
* Provide comprehensive documentation for model methodology and limitations.
* Establish monitoring guidelines for ongoing model performance tracking.

**Key Assumptions for Success:**

**1.Data quality consistency**: Production data will maintain the same quality standards as training data.

**2.Regulatory approval: Model** approach will meet insurance regulatory requirements without major modifications.

**3.User adoption**: Underwriters will trust and effectively utilize model recommendations in their decision-making.

**4.Infrastructure readiness:** Existing IT systems can support additional computational and storage requirements.

**5.Business stability**: Claim rate targets remain valid business objectives throughout implementation.

**Question 4: Assuming that the team you're working in only consists of data scientists, which other teams in the business would you need to speak to?**

**Answer:**

**Technology and Engineering Teams**

**1.MLOps/DevOps Engineers**

* Infrastructure management: Cloud deployment, server provisioning, auto-scaling setup.
* Pipeline automation: CI/CD implementation with GitHub Actions, deployment orchestration.
* Monitoring systems: Performance tracking, alerting, log management.
* Security implementation: Authentication, data encryption, access controls.

**2.Data Engineering Team**

* ETL pipeline development: Airflow DAG creation, data transformation logic.
* Database management: PostgreSQL optimization, backup strategies, data governance.
* Data quality assurance: Validation rules, monitoring systems, data lineage tracking.
* Feature store management: Schema design, performance optimization, data cataloging.

**3.Business and Stakeholder Teams**

* Process integration: Workflow design, business rule validation.
* User acceptance testing: Interface validation, training requirements.
* Business logic validation: Risk assessment rules, threshold optimization.

**Question 5: What is in scope and out of scope for your responsibility?**

**Answer:**

**In Scope - Data Science Team Responsibilities**

**1.Model Development and Maintenance:**

* Algorithm development: Model selection, feature engineering ad model training and hyperparameter tuning.
* Code architecture: Refactoring notebook code into modular OOP classes and design patterns.
* Performance optimization: Accuracy improvement, efficiency enhancement, scalability considerations.
* Model validation: Statistical testing, cross-validation, performance benchmarking
* Research and development: Exploring new algorithms, staying current with industry advances.

**2.Technical Documentation and Communication:**

* Model methodology documentation: Algorithm explanations, assumptions, limitations, interpretation guides.
* Performance reporting: Accuracy metrics, business impact analysis, recommendation summaries.
* Knowledge transfer: Documentation for other teams, troubleshooting guides, best practices.

**3.Monitoring and Analysis:**

* Performance tracking: Model accuracy monitoring using MLflow, prediction quality assessment.
* Business impact analysis: Claim rate tracking, target achievement measurement.
* Retraining recommendations: Performance degradation identification, update scheduling.
* Continuous improvement: Model enhancement identification, optimization opportunities.
* Deployment automation: CI/CD pipeline maintenance with GitHub Actions, release management.

**Out of Scope - Other Teams' Responsibilities**

**1.Infrastructure and Operations (DevOps/MLOps):**

* Server management: Hardware provisioning, OS maintenance, security patching
* System scaling: Load balancing, auto-scaling configuration on AWS/Azure, performance optimization
* Infrastructure monitoring: System health, resource utilization, capacity planning

**2.Business Process Integration (Operations Teams):**

* Workflow redesign: Business process changes, staff role modifications
* Change management: Organizational adoption, resistance management
* Operational procedures: Standard operating procedures, quality assurance processes

**3.Regulatory and Legal Management (Compliance):**

* Regulatory submissions: Model approval applications, compliance reporting
* Legal risk management: Liability assessment, contract negotiations
* Audit coordination: External audit management, regulatory examinations
* Policy development: Compliance policies, governance frameworks