

Suplemento Técnico: Dominio 2

Estrategias de Selección, GANs y Operaciones Avanzadas

Material de Estudio Complementario

1. Selección Estratégica de Modelos Fundacionales (FM)

La elección del modelo impacta directamente en la rentabilidad, la experiencia de usuario y la viabilidad técnica.

1.1. Criterios de Selección

- **Tamaño del Modelo:** Definido por el recuento de parámetros. Los modelos más grandes tienen más "memoria" pero mayor latencia y coste.
- **Ventanas de Contexto:** Determinan cuánta información puede procesar el modelo en un solo prompt (ej. resumir un libro completo vs. una página).
- **Opciones de Inferencia:** Elección entre llamadas a API (gestión simplificada) o despliegue autogestionado (mayor control y privacidad).
- **Modelos Específicos (Purpose-built):** Surgimiento de modelos más pequeños (1B - 40B parámetros) optimizados para tareas concretas (marketing, medicina), que ofrecen rendimiento comparable a modelos gigantes con menor gasto de recursos.

1.2. Benchmarks y Evaluación

- **Benchmarks Generalizados:** Como HELM (Stanford), útiles como punto de partida.
- **Benchmarks Personalizados:** Esenciales para casos de uso específicos (ej. resúmenes médicos). Se utilizan métricas como **BLEU** y **ROUGE** para cuantificar la calidad frente a referencias humanas.

2. Redes Generativas Antagónicas (GAN)

Arquitectura de aprendizaje no supervisado basada en la competición de dos redes neuronales.

2.1. Componentes y Funcionamiento

1. **Generador:** Crea datos falsos (imágenes, audio) intentando imitar el dataset original.
2. **Discriminador:** Actúa como un "juez" que intenta distinguir entre los datos reales y los generados por el generador.

El sistema alcanza el éxito cuando el discriminador ya no puede distinguir el dato sintético del original (estado de equilibrio).

2.2. Tipos de GAN y Aplicaciones

- **SRGAN (Super Resolution):** Mejora la resolución de imágenes de baja calidad.
- **CGAN (Conditional):** Genera datos basados en etiquetas específicas (ej. "genera un perro").
- **Aplicaciones:** Síntesis de video, aumento de datos sintéticos para entrenar otros modelos y restauración de imágenes médicas.

3. IA Agéntica (Agentic AI)

Representa el paso de la IA como herramienta a la IA como **colaborador autónomo**.

- **Definición:** Sistemas con capacidad de actuar independientemente, perseguir metas complejas, planificar pasos múltiples y aprender de los resultados.
- **Diferencia con IA Estrecha:** No solo ejecuta una tarea cuando se le pide; evalúa estrategias y se adapta a entornos dinámicos.
- **Casos de Uso:** Diseño arquitectónico generativo (optimización solar, materiales), planificación urbana autónoma y gestión de construcción en tiempo real.

4. Monitorización y Observabilidad en AWS

El uso de modelos fundacionales en producción requiere una vigilancia estricta mediante **Amazon Bedrock** y **Amazon CloudWatch**.

4.1. Métricas de Invocación y Rendimiento

- **Invocations:** Número de solicitudes a la API.
- **InvocationLatency:** Tiempo de respuesta del modelo.
- **Token Count:** Seguimiento de tokens de entrada y salida (crucial para el control de costes).

4.2. Logging y Protección de Datos

- **Model Invocation Logging:** Permite recolectar metadatos, prompts y respuestas. Se pueden enviar a S3 o CloudWatch Logs.
- **CloudWatch Logs Insights:** Permite analizar patrones en los prompts y detectar tendencias.
- **Protección de Datos Sensibles:** CloudWatch utiliza ML para detectar y enmascarar automáticamente información sensible (como direcciones IP o PII) en los logs antes de ser almacenados.

5. Marcos de Adopción Estratégica

- **CAF-AI (Cloud Adoption Framework for AI):** Guía para que las organizaciones generen valor de negocio, estructurando el viaje desde la madurez técnica inicial hasta la escala empresarial.
- **Well-Architected Framework (ML Lens):** Proporciona mejores prácticas para diseñar sistemas de ML seguros, eficientes y rentables en la nube de AWS.