Assignment 1: Survey of Failure Modes in Machine Learning Systems

1. Overview

You will survey credible sources (research papers, engineering blogs, whitepapers, documentation) to identify and explain common failure modes, realistic scenarios where they arise, and high-level mitigation ideas.

2. Deliverable and Submission

- A single pdf, not more than 6 pages with proper references. NAme the pdf firstname_lastname.pdf

3. Task Requirements

You must identify **at least 5 distinct ways** that ML systems can fail in real-world settings. For **each failure mode**, include all items below.

3.1. Per-Failure-Mode Checklist (Required)

For each failure mode, provide:

1. **Name of failure mode** (e.g., training–serving skew, data leakage, input drift).
2. **Definition:** a clear description in your own words.
3. **How/why it arises:** typical causes and conditions that trigger it.
4. **Scenario/example:** a realistic case where it occurs (industry example, paper case, or a plausible system).
5. **High-level mitigation ideas:** conceptual strategies (e.g., validation, monitoring, governance, separation of concerns).
6. **At least one citation** to a credible source supporting the failure mode and/or example.

4. Important: What Counts as "Mitigation"

Miitigation is not tools but ideas or concepts. Do not say:

> "Use Tool X to solve it."

Instead, use statements like:

"Introduce data validation gates that block training when schema changes or missingness exceeds a threshold,"
"Monitor feature distribution shifts and set escalation policies,"
"Reduce coupling by standardizing feature definitions and documenting downstream consumers."

5. Suggested Failure Modes (Non-Exhaustive)

You may include (but are not limited to):

- Input data drift / distribution shift
- Concept drift
- Training–serving skew
- Data leakage
- Poor data quality / label noise
- Hidden technical debt in ML systems
- Glue code

You are encouraged to go beyond this list if you find other well-supported failure modes.

6. Acceptable Sources

Use credible sources such as:

- Peer-reviewed research papers and surveys
- Conference papers / technical reports
- Industry engineering blogs (technical posts from reputable organizations)
- Whitepapers, standards, and official documentation
- Books or book chapters from established publishers

Avoid relying on:

- Anonymous or unverifiable blog posts
- Pure marketing content
- Sources that do not provide enough detail to support your claims
- NO medium article, weird website blogs etc.

7. Recommended Structure (Template)

You may follow this structure:

1. **Title + Your name**
2. **Introduction** (0.5–1 page): What MLOps is and why failure modes matter

3. **Failure Modes (5 sections)**: one subsection per failure mode using the checklist
4. **Synthesis / Discussion** (0.5–1 page): patterns you observed (e.g., data issues dominate)
5. **References**

8. Grading Rubric (100 Points)

1. **Coverage of failure modes (20 pts)**
   Meets or exceeds the requirement of 5 distinct failure modes; each is clearly distinct and well-labeled.
2. **Technical understanding and correctness (25 pts)**
   Explanations are accurate, clear, and demonstrate understanding of why the failure occurs.
3. **Scenarios and examples (20 pts)**
   Examples are realistic, well-explained, and clearly connected to the failure mode.
4. **Mitigation reasoning (15 pts)**
   Proposed mitigations are high-level, conceptually sound, and directly address the root causes (not just symptoms).
5. **Use of sources and citations (10 pts)**
   Uses credible sources; citations are complete, consistent, and correctly mapped in the References section.
6. **Organization and clarity (5 pts)**
   Well-structured, easy to follow, appropriate headings, and coherent flow.
7. **Writing quality (5 pts)**
   Grammar, readability, and professional tone.

9. Academic Integrity and Oral/Follow-Up Verification

This assignment must be completed **individually**. You must properly cite all external sources and write explanations in your own words.

Verification clause: After submission, I reserve the right to ask you **oral and/or written follow-up questions** about any part of your submission. If you cannot reasonably explain the work you submitted (including your chosen failure modes, examples, and mitigations), I may assign academic penalties up to and including a zero grade.

Misconduct: Plagiarism, fabricated citations, misrepresentation of sources, or submitting work you do not understand will be treated as academic misconduct. I reserve the right to penalize such cases in any way I deem fit.