Quiz: Adversarial Robustness and Regulatory Readiness

Section 05 – Digital-AI-Finance

Joerg Osterrieder

Zurich University of Applied Sciences (ZHAW)

2025

Question 1: Attack Vectors

How many adversarial attack vectors are identified?

a) 2
b) 3
c) 4
d) 5

Question 1: Attack Vectors

How many adversarial attack vectors are identified?

a) 2
b) 3
c) 4
d) 5

Answer

c) 4
Four principal attack vectors are identified: data poisoning, evasion attacks, model extraction, and strategic timing and regime exploitation.

Source: Section 5.1

Question 2: Mean AUC Degradation

What is the mean AUC degradation under adversarial attack?

a) 5.3%
b) 8.2%
c) 10.6%
d) 15.4%

Question 2: Mean AUC Degradation

What is the mean AUC degradation under adversarial attack?

a) 5.3%

b) 8.2%

c) 10.6%

d) 15.4%

Answer

c) 10.6%

Recent work on adversarial robustness in financial ML reports a mean AUC degradation of 10.6% across surveyed detection systems under adversarial attack.

Source: Section 5.1

Question 3: Adversarial Training Recovery

How much AUC does adversarial training recover?

a) 30–40%
b) 45–55%
c) 60–70%
d) 80–90%

Question 3: Adversarial Training Recovery

How much AUC does adversarial training recover?

a) 30–40%
b) 45–55%
c) 60–70%
d) 80–90%

Answer

c) 60–70%
Robust optimization applied to financial fraud detection models can recover 60–70% of the AUC lost to adversarial attacks, reducing attack success rates from approximately 35% to 5%.

Source: Section 5.2

Question 4: EU AI Act Transparency

Which EU AI Act article addresses transparency?

a) Article 9
b) Article 13
c) Article 14
d) Article 52

Question 4: EU AI Act Transparency

Which EU AI Act article addresses transparency?

a) Article 9
b) Article 13
c) Article 14
d) Article 52

Answer

b) Article 13
Article 13 of the EU AI Act mandates transparency: high-risk AI systems must be designed to enable users to interpret the system's output and use it appropriately.

Source: Section 5.3

Question 5: EU AI Act Oversight

Which EU AI Act article addresses human oversight?

a) Article 9
b) Article 13
c) Article 14
d) Article 52

Question 5: EU AI Act Oversight

Which EU AI Act article addresses human oversight?

a) Article 9
b) Article 13
c) Article 14
d) Article 52

Answer

c) Article 14
Article 14 of the EU AI Act requires human oversight: high-risk systems must allow effective oversight by natural persons, including the ability to override the system's output.

Source: Section 5.3

Question 6: Institutional Preparedness

What percentage of institutions lack adversarial resilience policies?

a) 45%
b) 58%
c) 68%
d) 78%

Question 6: Institutional Preparedness

What percentage of institutions lack adversarial resilience policies?

a) 45%
b) 58%
c) 68%
d) 78%

Answer

d) 78%
A survey of financial institutions found that 78% lacked formal adversarial resilience policies for their ML-based detection systems, suggesting a wide gap between threat landscape and preparedness.

Source: Section 5.1

Question 7: Data Poisoning Impact

What is the data poisoning degradation range?

a) 1–3%
b) 5–12%
c) 15–25%
d) 30–40%

Question 7: Data Poisoning Impact

What is the data poisoning degradation range?

a) 1–3%
b) 5–12%
c) 15–25%
d) 30–40%

Answer

b) 5–12%
Data poisoning attacks can degrade model performance by 5–12% even when the fraction of poisoned samples is small, particularly concerning given class imbalance amplifies the impact of corrupted labels.

Source: Section 5.1