EXAM PROFESSIONAL MACHINE LEARNING ENGINEER TOPIC 1 QUESTION 205 DISCUSSI...

Actual exam question from Google's Professional Machine Learning Engineer
Question #: 205
Topic #: 1
[All Professional Machine Learning Engineer Questions]

You are analyzing customer data for a healthcare organization that is stored in Cloud Storage. The data contains personally identifiable information (PII). You need to perform data exploration and preprocessing while ensuring the security and privacy of sensitive fields. What should you do?

A. Use the Cloud Data Loss Prevention (DLP) API to de-identify the PII before performing data exploration and preprocessing.

B. Use customer-managed encryption keys (CMEK) to encrypt the PII data at rest, and decrypt the PII data during data exploration and preprocessing.

C. Use a VM inside a VPC Service Controls security perimeter to perform data exploration and preprocessing.

D. Use Google-managed encryption keys to encrypt the PII data at rest, and decrypt the PII data during data exploration and preprocessing.

Show Suggested Answer

by pikachu007 at *Jan. 13, 2024, 4:35 a.m.*

Comments

Type your comment...

Submit

fitri001 6 months, 2 weeks ago

Selected Answer: A

Cloud DLP API: This service redacts or replaces sensitive information in your data before processing. It allows data exploration and analysis without exposing PII directly.
Privacy Preservation: De-identification ensures sensitive information is not revealed during analysis, protecting patient privacy.

upvoted 2 times

fitri001 6 months, 2 weeks ago

B. CMEK and decryption: While CMEKs provide strong encryption, decrypting PII data during exploration exposes sensitive information. This increases the risk of accidental leaks or unauthorized access.
C. VM with VPC Service Controls: This approach can add complexity and doesn't directly address PII privacy concerns during analysis.
D. Google-managed encryption and decryption: Similar to option B, decrypting PII data for exploration weakens privacy.

upvoted 1 times

pinimichele01 7 months ago

Selected Answer: A

https://cloud.google.com/dlp/docs/inspect-sensitive-text-de-identify

upvoted 1 times

edoo 8 months ago

Selected Answer: A

A is obvious.

upvoted 1 times

b1a8fae 9 months, 3 weeks ago

Selected Answer: A

A. https://cloud.google.com/dlp/docs/inspect-sensitive-text-de-identify

upvoted 1 times

pikachu007 9 months, 3 weeks ago

Selected Answer: A

Minimizes exposure of sensitive data: De-identification replaces or removes sensitive information, reducing the risk of accidental exposure or unauthorized access during analysis.
Preserves data utility: DLP can de-identify data while maintaining its usefulness for exploration and preprocessing, ensuring meaningful analysis without compromising privacy.
Flexibility in de-identification: You can choose appropriate de-identification techniques (e.g., masking, pseudonymization, generalization) based on specific privacy requirements and analysis needs.

upvoted 2 times

Facebook , Twitter
YouTube , Reddit
Pinterest

We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.