EXAM PROFESSIONAL MACHINE LEARNING ENGINEER TOPIC 1 QUESTION 107 DISCUSSI...

Actual exam question from Google's Professional Machine Learning Engineer
Question #: 107
Topic #: 1
[All Professional Machine Learning Engineer Questions]

You are an ML engineer at a bank that has a mobile application. Management has asked you to build an ML-based biometric authentication for the app that verifies a customer's identity based on their fingerprint. Fingerprints are considered highly sensitive personal information and cannot be downloaded and stored into the bank databases. Which learning strategy should you recommend to train and deploy this ML mode?

A. Data Loss Prevention API

B. Federated learning

C. MD5 to encrypt data

D. Differential privacy

Show Suggested Answer

by mil_spyro at *Dec. 13, 2022, 9:52 p.m.*

Comments

Type your comment...

Submit

hiromi Highly Voted 1 year, 10 months ago

Selected Answer: B

B
With federated learning, all the data is collected, and the model is trained with algorithms across multiple decentralized edge devices such as cell phones or websites, without exchanging them.
(Journey to Become a Google Cloud Machine Learning Engineer: Build the mind and hand of a Google Certified ML professional)

upvoted 9 times

fitri001 Most Recent 6 months, 2 weeks ago

Selected Answer: B

Federated learning allows training the model on the user's devices themselves.

pen_spark
expand_more The model updates its parameters based on local training data on the device without ever needing the raw fingerprint information to leave the device. This ensures the highest level of privacy for sensitive biometric data.

upvoted 1 times

fitri001 6 months, 2 weeks ago

Data Loss Prevention API (DLAPI): This focuses on protecting data at rest and in transit, not relevant to training a model without storing data.
MD5 Encryption: This is a one-way hashing function, not suitable for encryption and decryption needed for training.expand_more
Differential privacy: While it adds noise to protect privacy, it's not ideal for training image recognition models like fingerprint identification.

upvoted 1 times

Voyager2 1 year, 5 months ago

B. Federated learning.
"information and cannot be downloaded and stored into the bank databases" That excludes DLP. ederated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device, decoupling the ability to do machine learning from the need to store the data in the cloud.

upvoted 2 times

M25 1 year, 6 months ago

Selected Answer: B

Went with B

upvoted 1 times

Yajnas_arpohc 1 year, 7 months ago

Selected Answer: B

I think the giveaway is in the question "Which learning strategy.."... Federated Learning seems to be the only one !

upvoted 3 times

TNT87 1 year, 8 months ago

Selected Answer: B

B. Federated learning would be the best learning strategy to train and deploy the ML model for biometric authentication in this scenario. Federated learning allows for training an ML model on distributed data without transferring the raw data to a centralized location.

upvoted 2 times

zzzzzooooo 1 year, 8 months ago

Selected Answer: A

Ans is A for me

upvoted 1 times

ares81 1 year, 10 months ago

Selected Answer: A

It seems A, to me.

upvoted 1 times

mil_spyro 1 year, 10 months ago

Selected Answer: B

Federated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device.
https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

upvoted 1 times

Social Media

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.