Privacy-Preserving AI
Hackathon

NEUROCRYPT

SIMON COESSENS
ARIJIT SAMAL
THOMAS CHARDONNENS
ANAND-ARNAUD PAJANIRADJANE
BATU ERGUN

yahoo!finance

Meta, Apple are investing in tech that can decode your thoughts

May 13

BBC

Neuralink: Can Musk's brain technology change the world?

Feb 3

WIRED

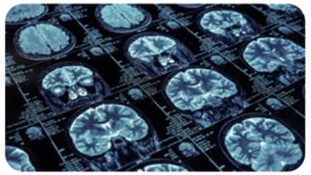
This Brain Implant Lets People Control Amazon Alexa With Their Minds

12 days ago • By Emily Mullin

CNBC

A wave of biological privacy laws may be coming as tech gadgets capture our brain waves

Aug 17



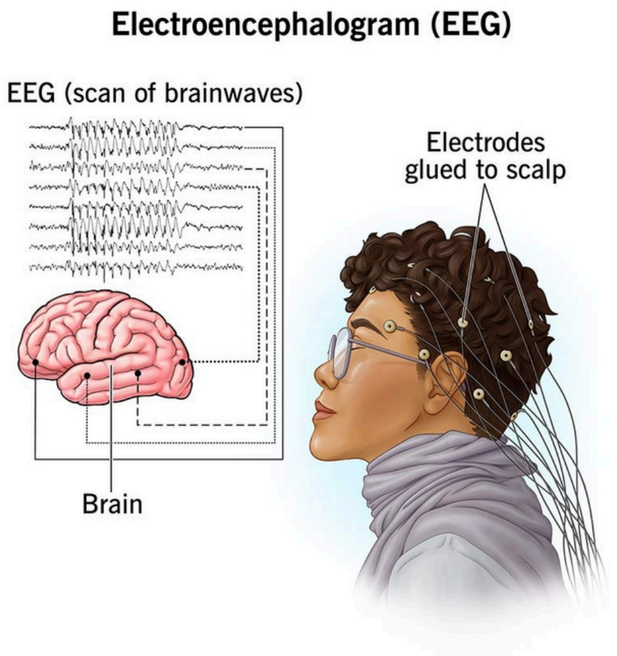
The Problem

EEG Brain waves contain useful but sensitive information

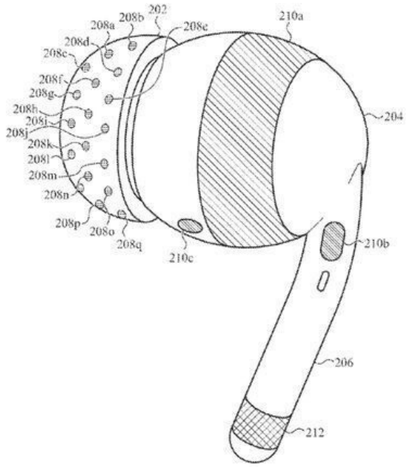
The devices measuring the waves don't have a lot of computing power and require low latency

FHE on cloud machine learning offers a solution here

What is EEG?

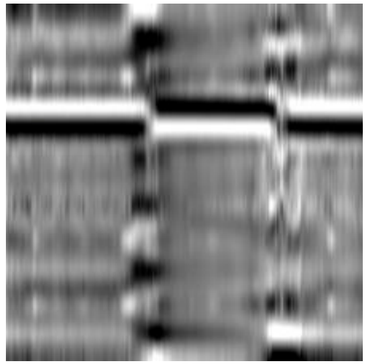


- *A method of recording electrical activity of the brain.*
- *Has a wide range of valuable applications:*
  - *Seizure detection*
  - *Brain-computer interfaces*
  - *Mental health monitoring*
- *Companies like Apple and Meta are making significant investments. But privacy?*



EEG enabled Airpods patent 2023

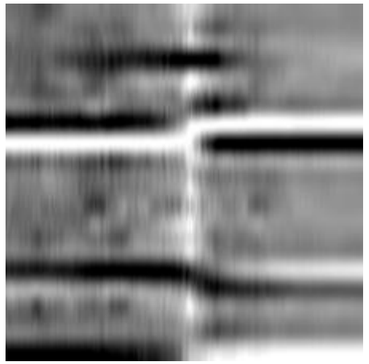
The Dataset



Seizure

KEY FEATURES

- *Image Size: 224x224 pixels*
- *Total Dataset Size: 1,318,793 rows*
- *Captured over 6-second windows*
- *Captures different brain wave frequencies*
- 🔗 🤗 *Seizure EEG Dataset*

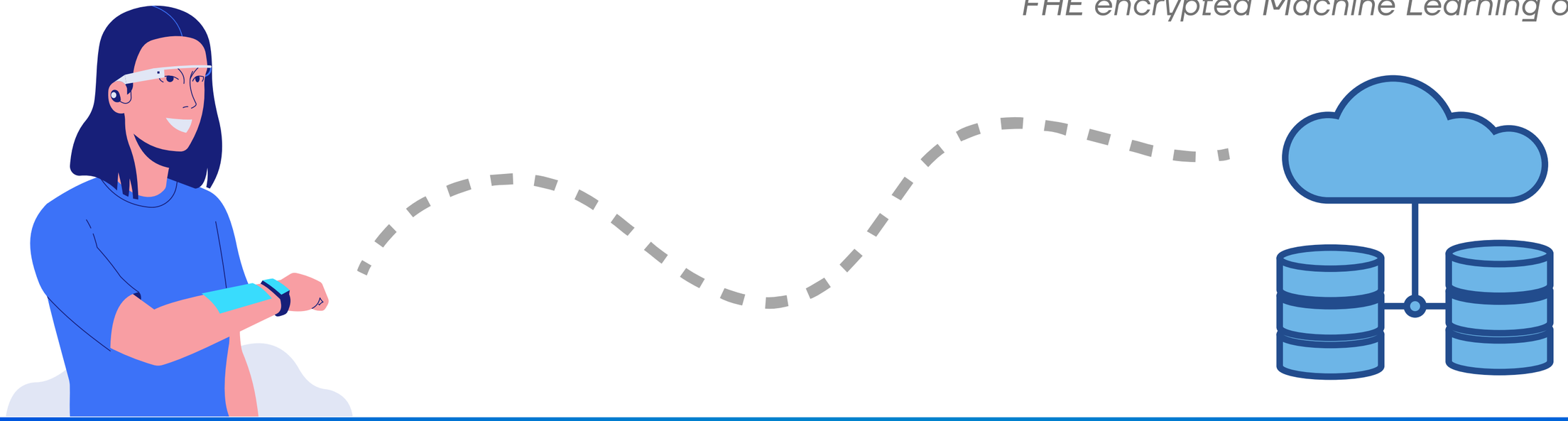


No seizure

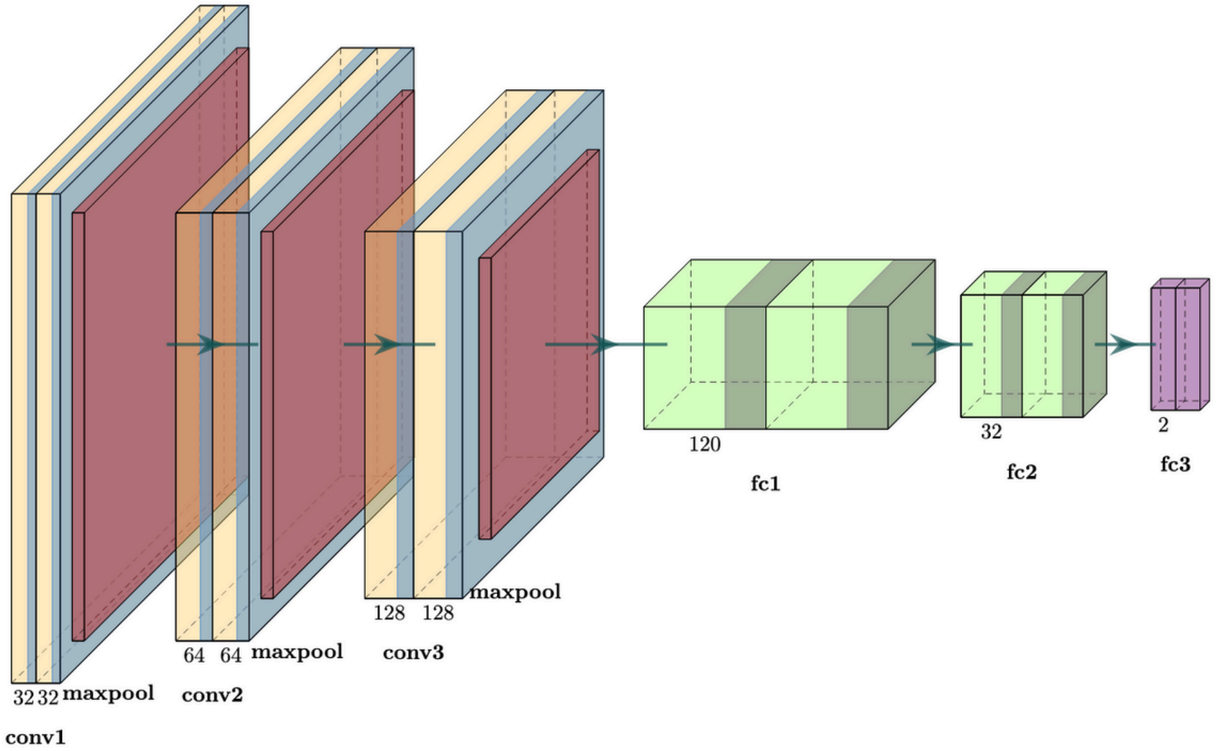
The Solution

A wearable device *on which Brain waves are FHE encrypted and send to the cloud*

FHE encrypted Machine Learning on the Cloud

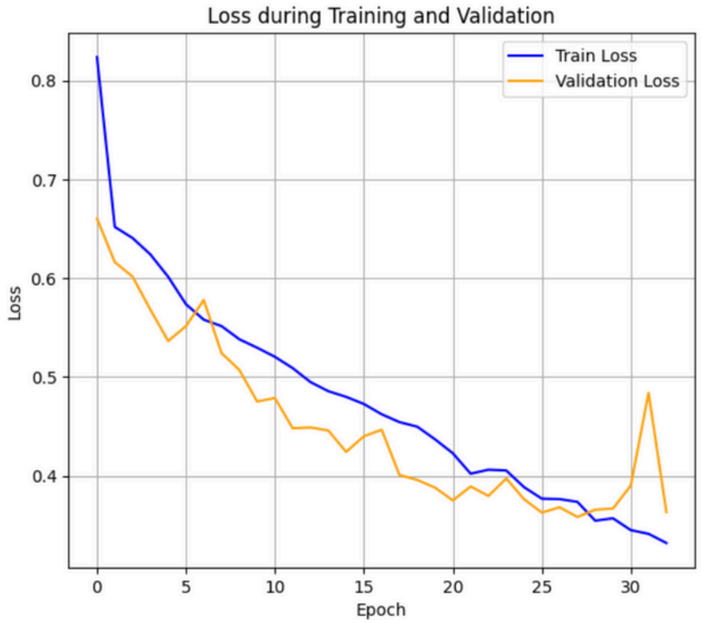


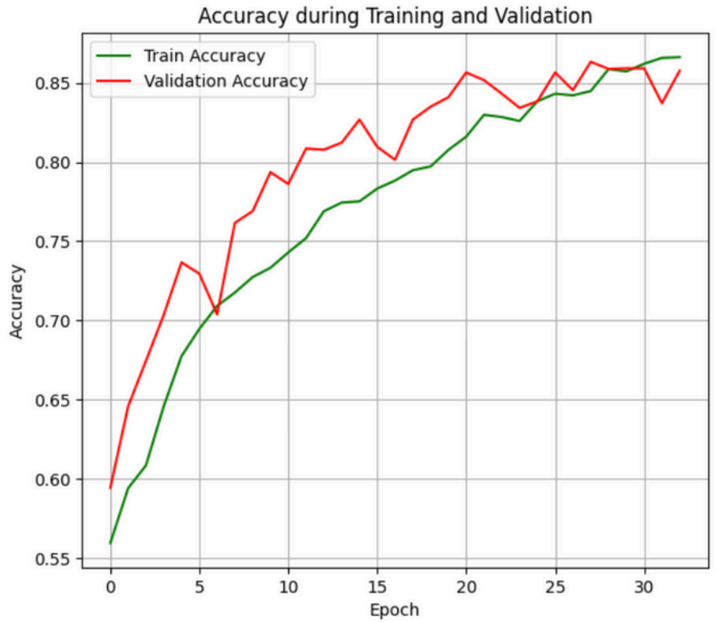
The Solution



- *Training statistics of the non-encrypted CNN*
- *Tested for 32x32 and 224x224*
- *Around 85% validation accuracy*
- *500k -> 70k -> 15k*

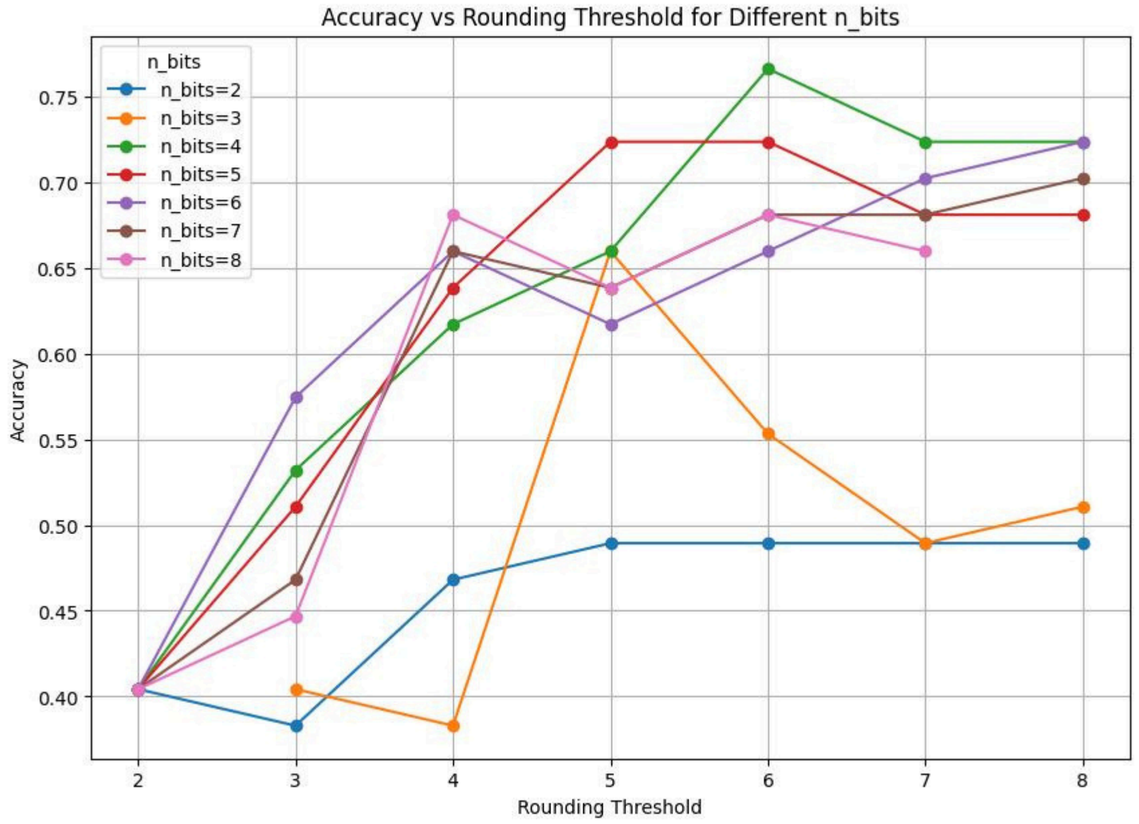
The Solution: Non-Encrypted





- *Training statistics of the non-encrypted CNN*
- *Tested for 32x32 and 224x224*
- *Around 80% validation accuracy*

The Solution: Encrypted



- *Post-Training Encryption with Concrete-ML*
- *Around 77% validation accuracy*
- *Both in simulate and execute mode [in 7min]*

The Demo


gBros
like 2
Running on L4
Logs
App
Seizure Detection on Encrypted EEG Data Using Fully Homomorphic Encryption
EEG image.
matically be resized to shape (32, 32). The image here, however, is displayed in its original resolution.
age here.
Examples to use.
the private key.
Generate the private key.
nerated:
e image using FHE.
Encrypt the image using FHE.

Privacy-Preserving AI
Hackathon

THANK YOU!

```
ValueError: Expected argument 0 to be EncryptedTensor but it's EncryptedTensor
```