Experts Live Kenya

EXPERTS LIVE KENYA

26TH JULY 2024
NAIROBI, KENYA

Experts Live Kenya

Privacy Preserving Framework for machine Learning on sensitive Data

Brackly Murunga
Machine Learning Engineer @ BAT

khanbrackly@gmail.com
+254 741 806 859

Agenda

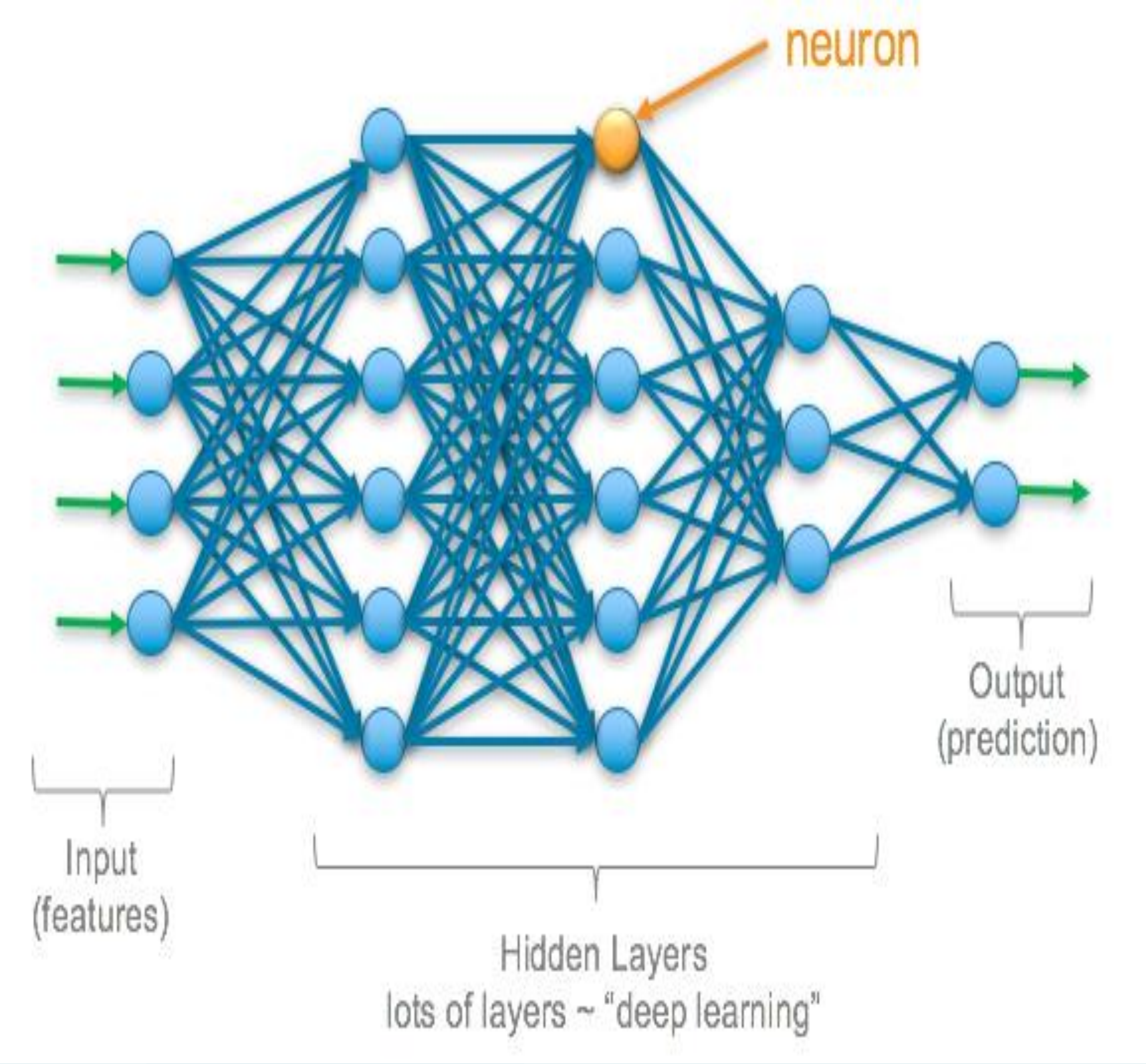
- Deep Learning : The One's and two's
- Sensitive Data: The tricky puzzle.
- Privacy toolkits in Machine Learning : The Fragile Tradeoff
- Latent representations: A magic wand.
- Azure ML Orchestration : Notebooks

Deep Learning Magic

The Ones and Twos

Deep Neural Networks

- ✓ **Are Powerful**: Can Approximate any function, Linear/ Non Linear
- ✓ **Are Data Hungry**. More Data better results.
- ✓ **This Ideology Gave rise to large scale pooling of Data**
    - ❖ ImageNet – Computer Vision
    - ❖ C4 dataset- Natural Language Processing



Data Pooling: Impact & Challenge

- Collaborative machine learning:
  - Better and more capable models
  - Rapid model development
- **Catch**: Possible with unsensitive data

Sensitive Data

The Tricky Puzzle

What constitutes sensitive Data?

Credits: https://www.polymerhq.io/blog/cloud-security/a-comprehensive-guide-to-defining-what-is-sensitive-data/

The Challenge of sensitive data

- Data Privacy and Legal Risks
- Data Governance Due to PII Data

Makes it hard to collaboratively share data between peers.

Privacy toolkits in Machine Learning

The Fragile Trade off

Experts Live Kenya

Federated Learning

- ✓ Local Training: Each device trains the model on its local data.
- ✓ Model Updates: After local training, each device sends the model updates to a central server.
- ✓ Aggregation: The central server aggregates the model updates from all participating devices to update the global Model.
- ✓ Iteration: This process iterates multiple times until the global model converges.

Differential Privacy

- ✓ Mathematical framework aimed at providing guarantees that the privacy of individuals in a dataset is preserved when statistical analyses are performed
- ✓ It ensures that the inclusion or exclusion of any single individual's data does not significantly affect the outcome of any analysis
- ✓ adding carefully calibrated random noise to the results of queries or analyses. This noise masks the contribution of individual data points, making it difficult for adversaries to infer sensitive information about any single individual from the published results.

Dimensionality Reduction (PCA)

- PCA reduces the number of dimensions in the data by transforming it into a new set of uncorrelated variables (principal components
- PCA can obscure specific sensitive details of the original data, as the principal components often do not directly correspond to individual data points
- The transformed data from PCA can act as an anonymized version of the original dataset

Latent Representations:

A Magic wand

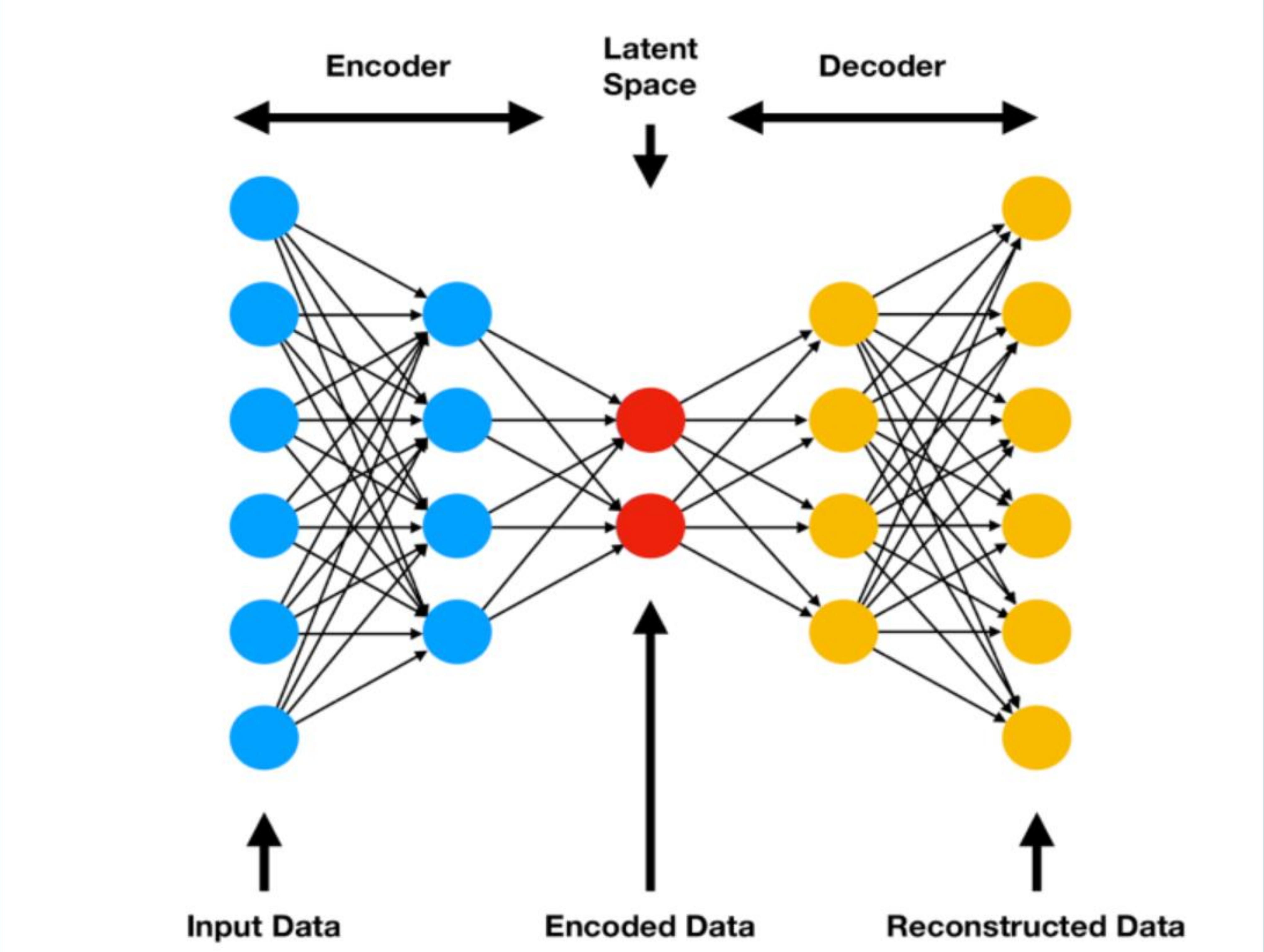
"To truly understand something, sometimes you need to take it apart and put it back together again."

Quote

Enter Auto Encoders…

An autoencoder is a specific type of a neural network, which is mainly designed to **encode** the input into a compressed and meaningful representation, and then **decode** it back such that the reconstructed input is similar as possible to the original one.

Bank et al (2021)



Experts Live Kenya

Latent Representation of Data

Dor Bank, Noam Koenigstein, Raja Giryes

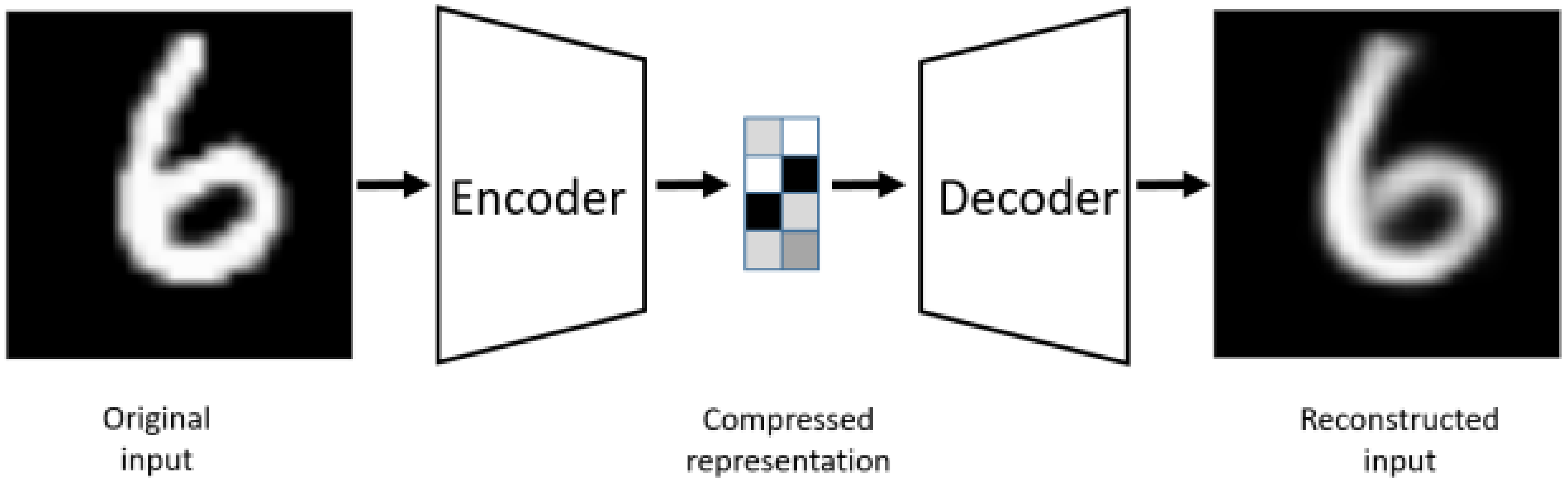


Fig. 1: An autoencoder example. The input image is encoded to a compressed representation and then decoded.

Experts Live Kenya

The Latent Space

- ✓ Lower Dimensionality
- ✓ Relatively unexplainable
- ✓ Noise Reduction
- ✓ Raw Data -> Feature Extraction -> Generalization

Taking the sensitive out of the Data.

State-gov	77516	Bachelors	13	Never-married	Adm-clerical	Not-in-family	White	Male	2174	0	40	United-States	<=50K	Set
Self-emp-not-inc	83311	Bachelors	13	Married-civ-spouse	Exec-managerial	Husband	White	Male	0	0	13	United-States	<=50K	train
Private	215646	HS-grad	9	Divorced	Handlers-cleaners	Not-in-family	White	Male	0	0	40	United-States	<=50K	train

↓

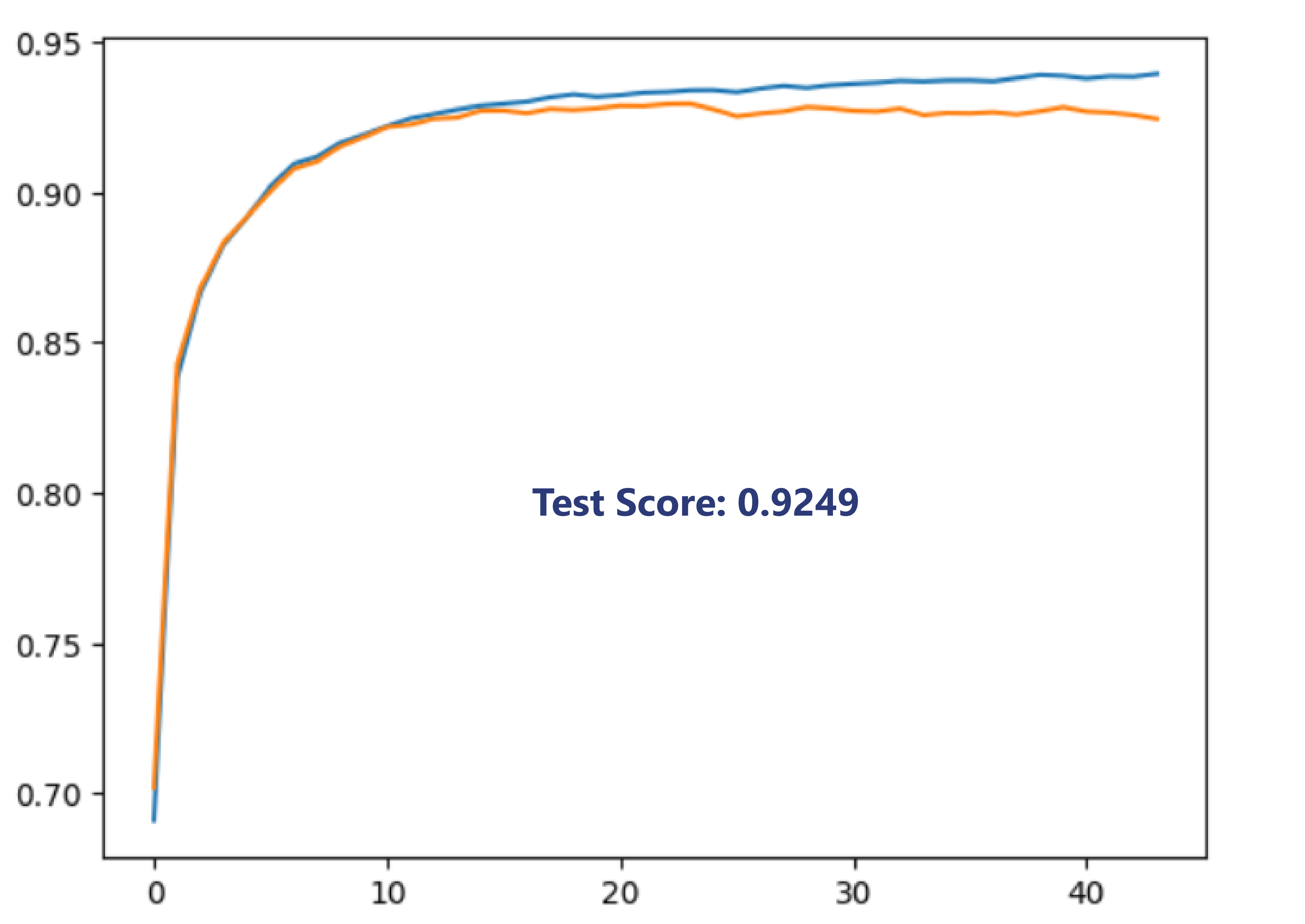
	latent_var1	latent_var2	latent_var3	latent_var4	latent_var5	Target
0	0.341742	-0.465697	0.037848	-0.023444	0.984669	not_wealthy
1	0.688599	-0.804189	-0.421492	-0.023444	0.984669	wealthy
2	0.614035	-0.642798	-0.226191	-0.023444	0.984669	not_wealthy
3	0.823717	-0.877059	-0.530586	-0.023444	0.984669	not_wealthy
4	-0.674778	0.546423	1.280261	-2.990632	-1.651739	wealthy

0.9249

Proof that it works

AUC of model trained with Raw Data

[<matplotlib.lines.Line2D at 0x7e9ae3f65d50>]



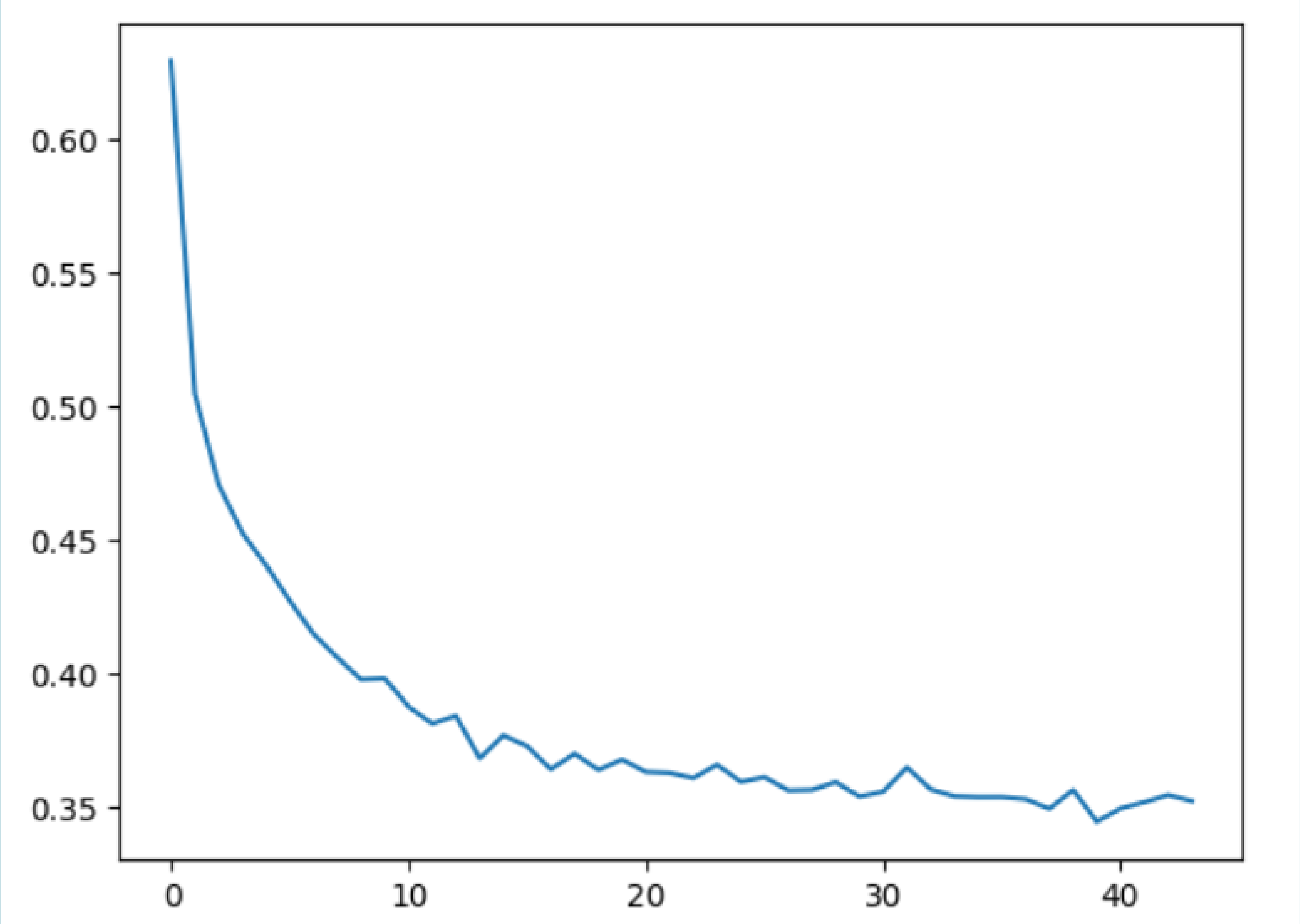
AUC of Model trained with Latent Representations

[<matplotlib.lines.Line2D at 0x7e9ae2e73be0>]

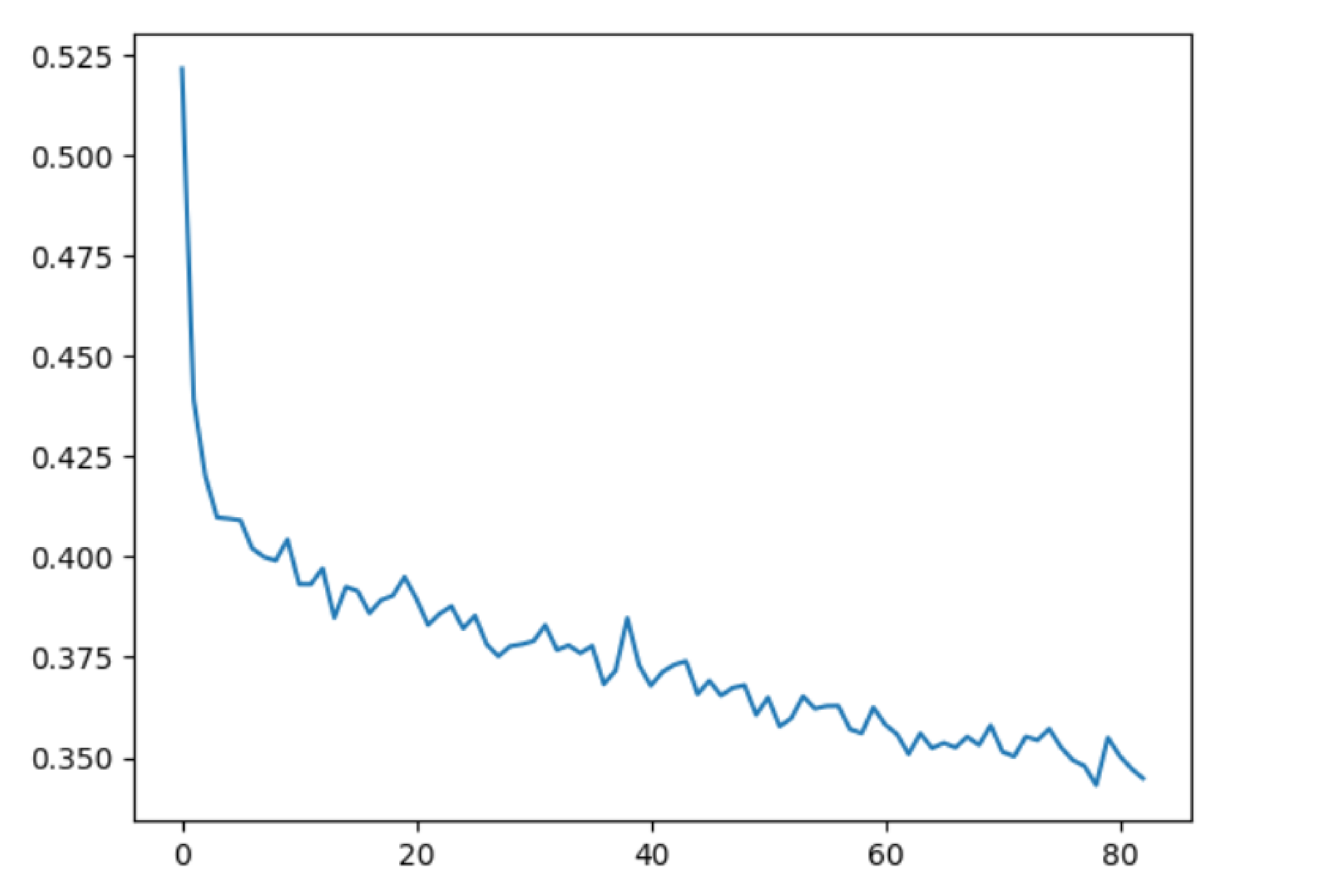
Experts Live Kenya

Proof that it works

Raw Data Model Loss



Latent Representations model Loss

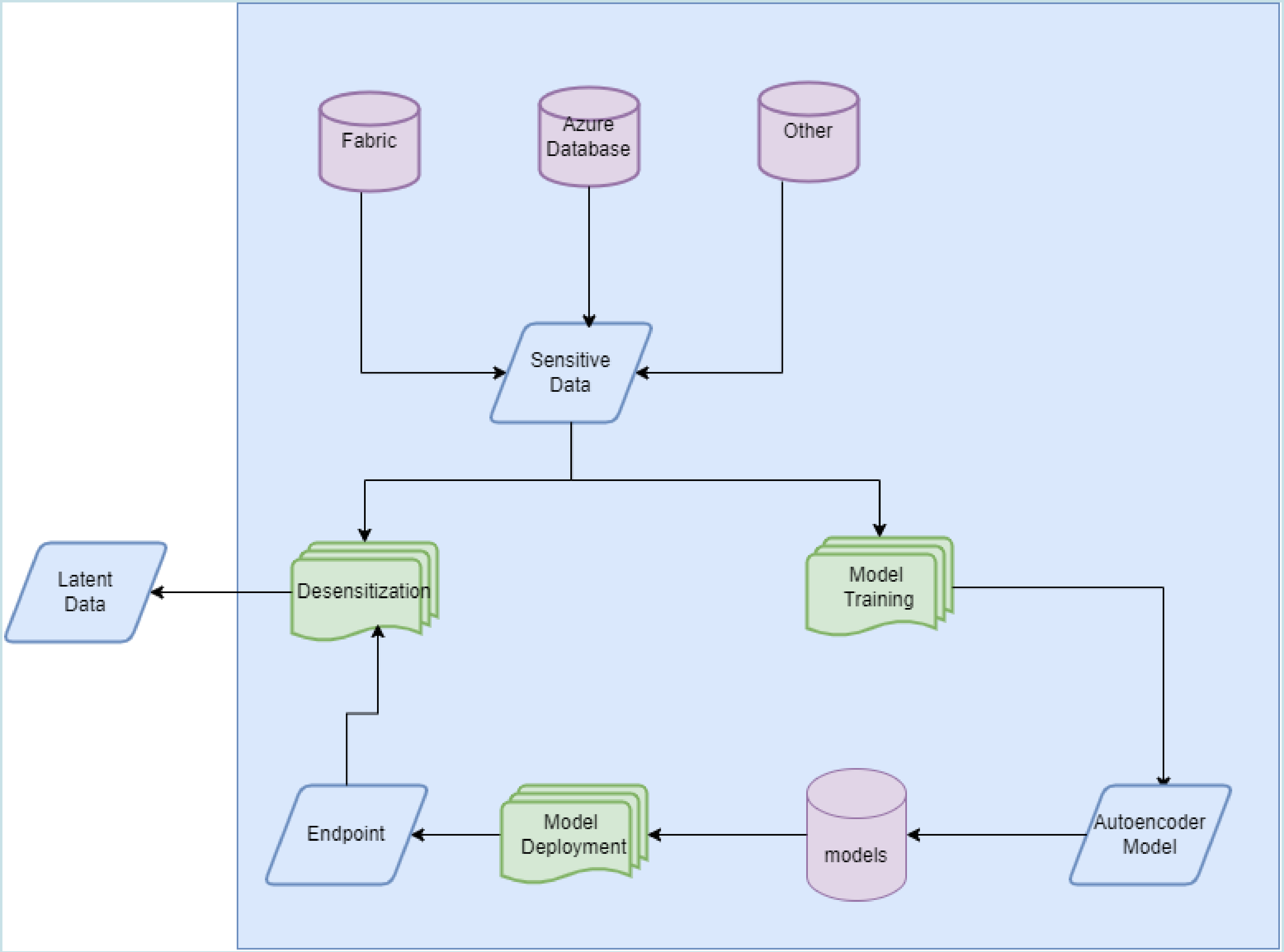


Different Use cases/ Scenarios

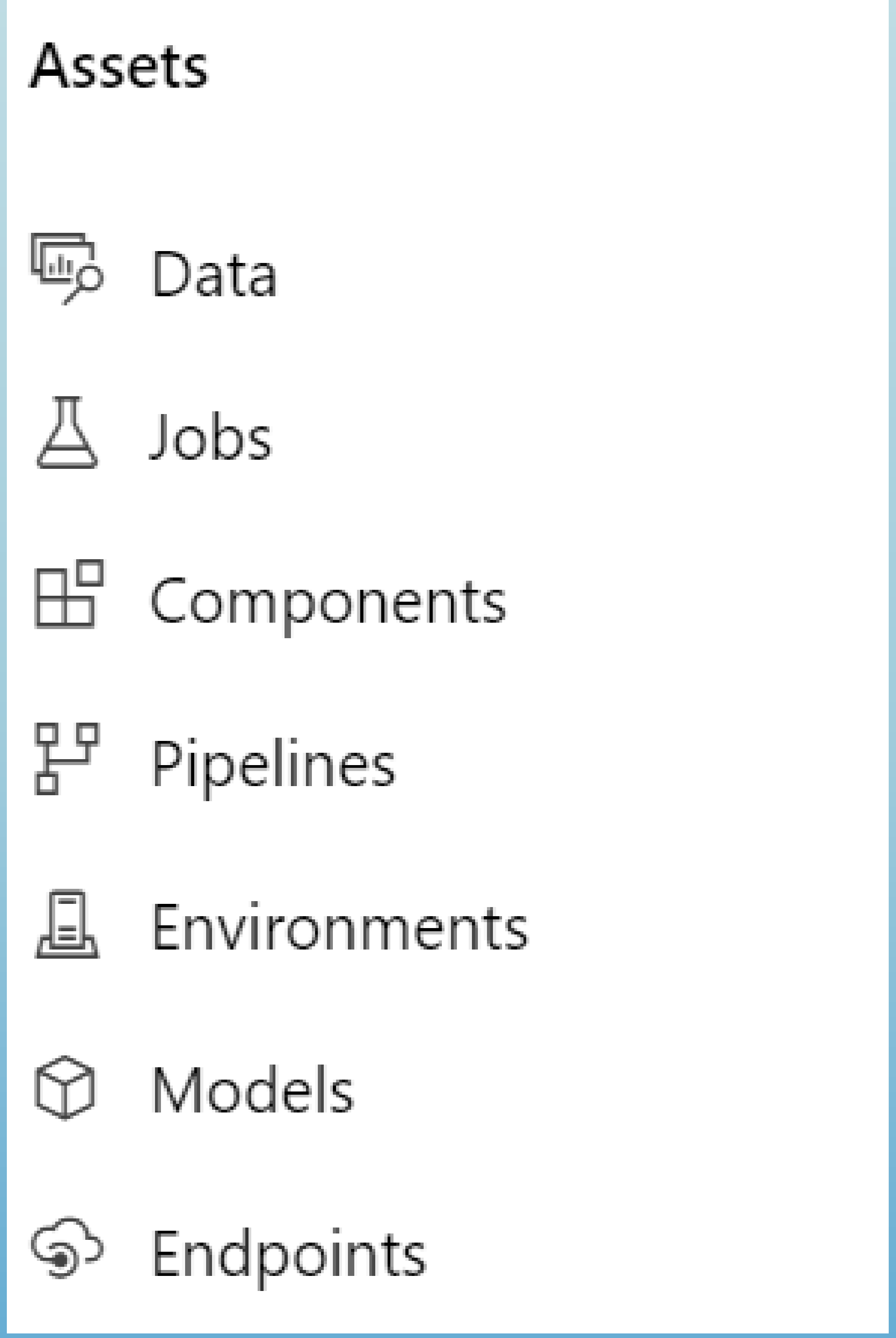
- ➢ Same features less/fragmented data.
- ➢ Different features same data – different parties collect different features of the same data

✓ ***Possibility of anonymization and collecting huge datasets***

Orchestration with Vs code & Azure ML:



Fabric
Azure Database
Other
Sensitive Data
Desensitization
Model Training
Latent Data
Endpoint
Model Deployment
models
Autoencoder Model



Assets
Data
Jobs
Components
Pipelines
Environments
Models
Endpoints

CODE

Ochestration Tools

- VS code /Azure Notebooks - Prototypying
- VS Code – Component
- Azure ML:
    - Components
    - Pipelines
    - Endpoints

Experts Live Kenya

CODE

https://github.com/Brackly/Privacy-ML

Conclusion

To truly understand something, sometimes you need to take it apart and put it back together again

Session Feedback

Session Track: DATA & AI

Session Name: Privacy preserving framework for machine learning on sensitive data.

THANK YOU

Speaker Name: Brackly Murunga
Speaker Title: Machine Learning Engineer
Speaker Social Media/links:

- Linkedin: Brackly Murunga
- Email: khanbrackly@gmail.com
- Phone: +254 741 806 859

THANK YOU TO OUR SPONSORS!