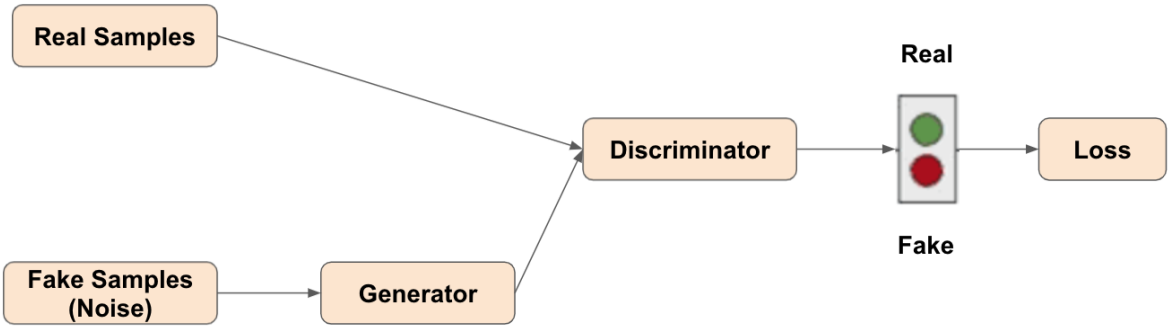
Assignment 4 - DL

Einat Shusterman 307848952
Moran Shemesh 301440285

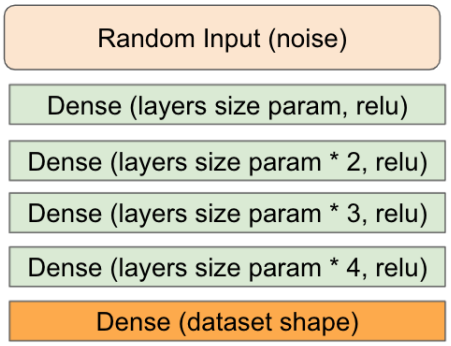
Preprocess step on both datasets:
Categorical features - we encode categorical features as to integer values. We encode the features to numerical values and are not using one hot encoding.
Continuous features - we kept the same.
We used PowerTransformer scaler (from Sklearn) on all the features to get a Gaussian distribution for the data.

Part 1 – Generative Adversarial Networks

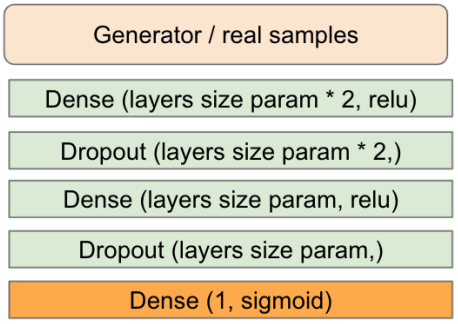
The architecture of the GAN:



The architecture of the Generator:



The architecture of the Discriminator:

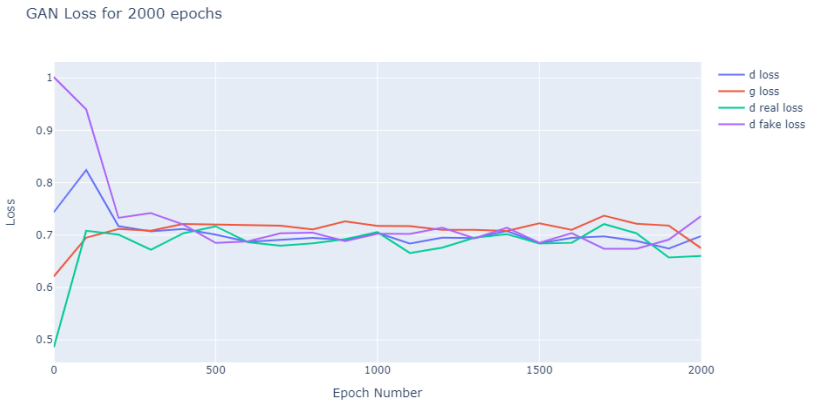


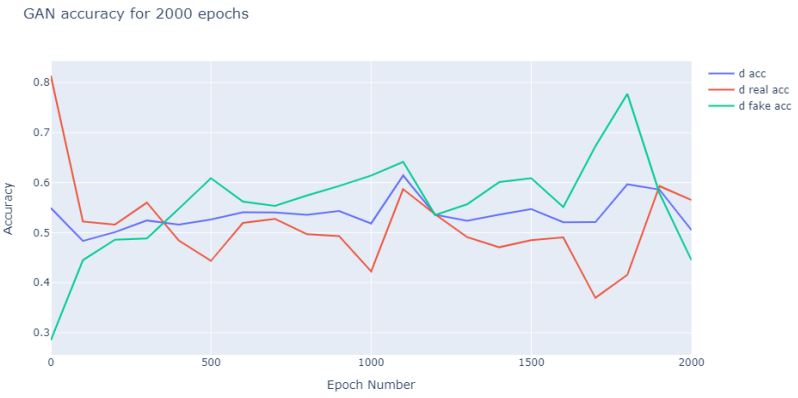
Results on Datasets:

1. **Diabetes Dataset:**
   Hyper parameters:

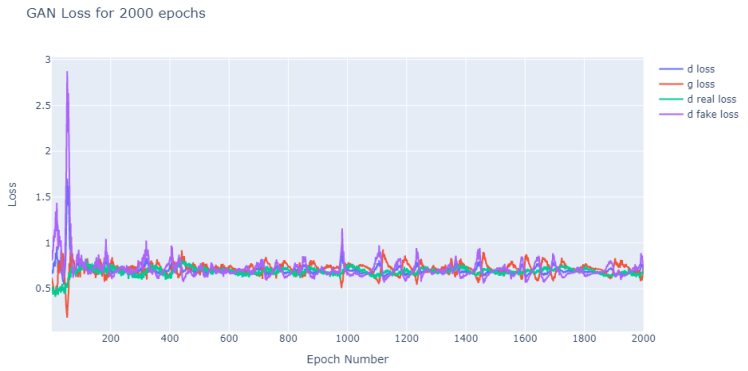
Parameter description	**Parameter value**
batch size	64
Number of epochs	2000
Learning rate	5e-4
Noise dimension size	32
Number of units in layers factor	30

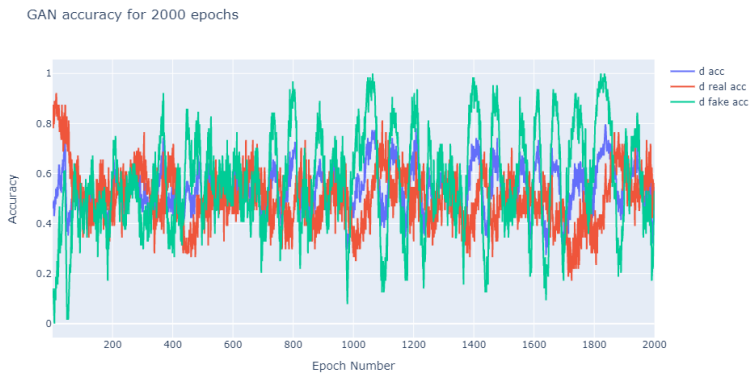
Average statistics per 100 epochs:





Raw statistics:

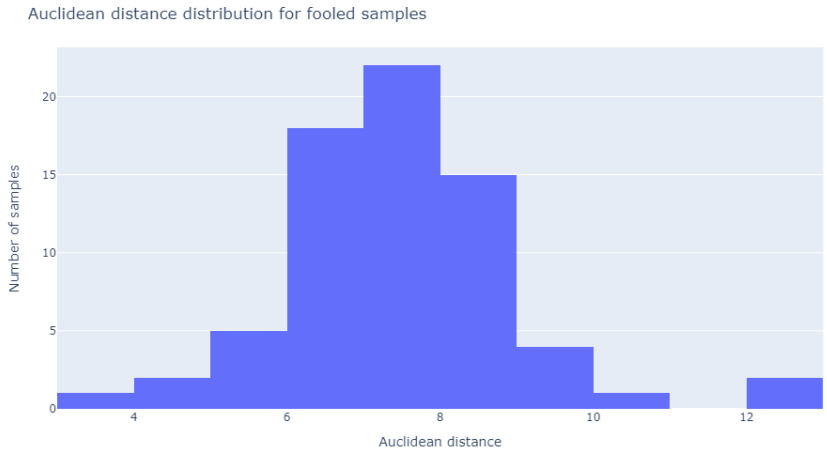




The GAN converged at epoch 2000.

<u>Samples that fooled the Discriminator:</u>

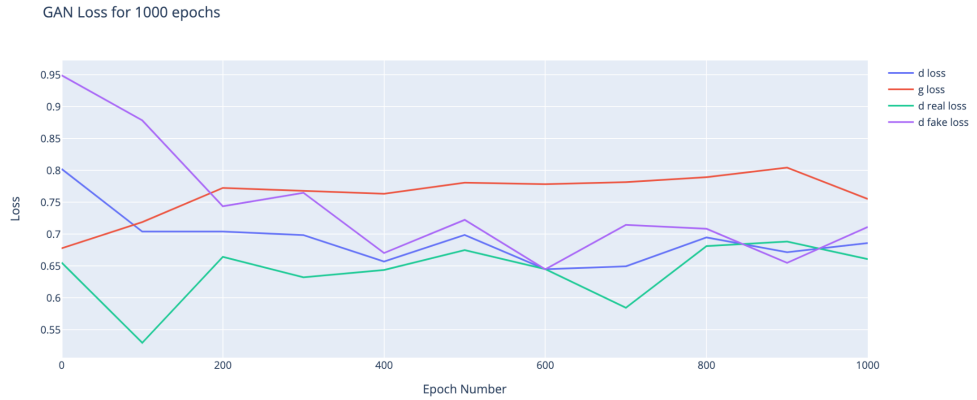
Out of 100 generated samples, 70 fooled the Discriminator, while 30 did not.

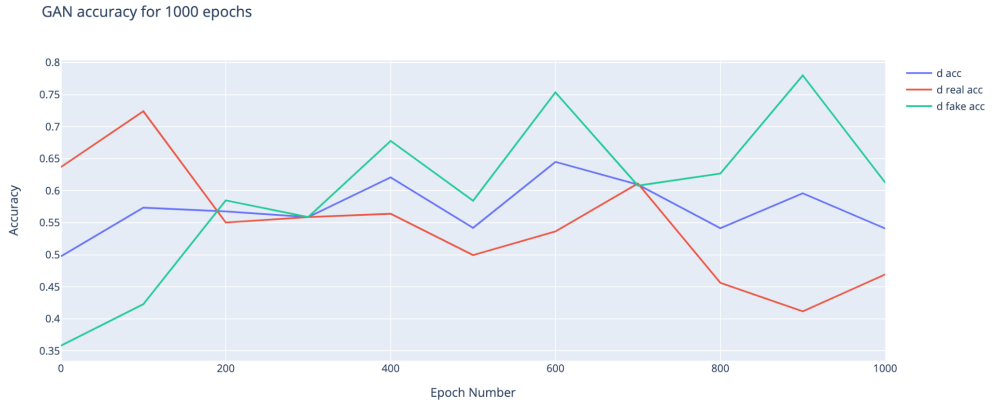


2. **German credit Dataset:**
   Hyper parameters:

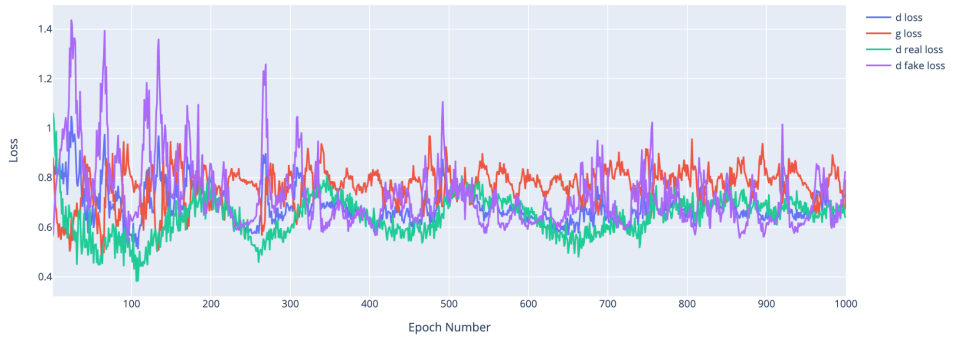
Parameter description	**Parameter value**
batch size	64
Number of epochs	1000
Learning rate	1e-3
Noise dimension size	64
Number of units in layers factor	25

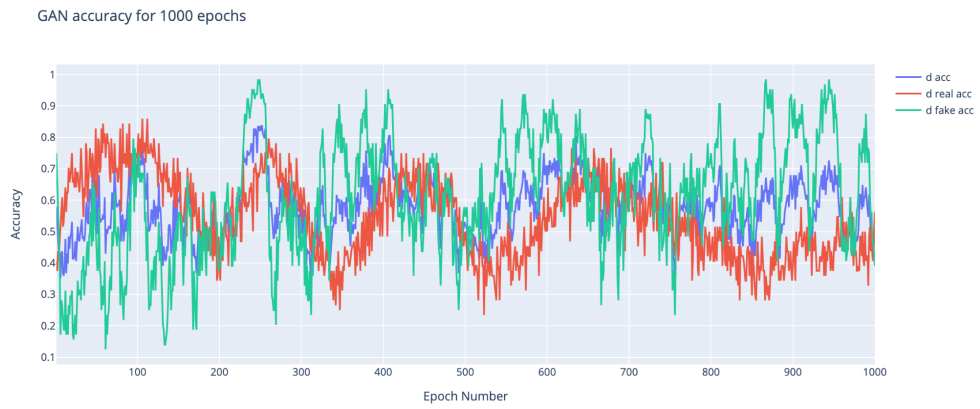
Average per 100 epoch





Raw statistics:

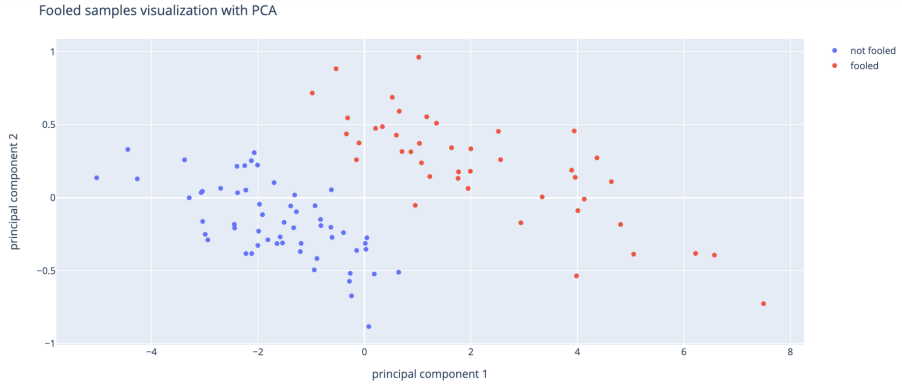


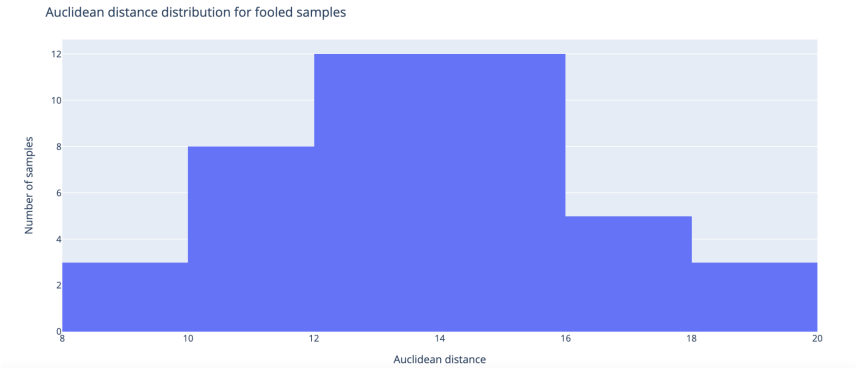


The GAN converged at epoch 1000.

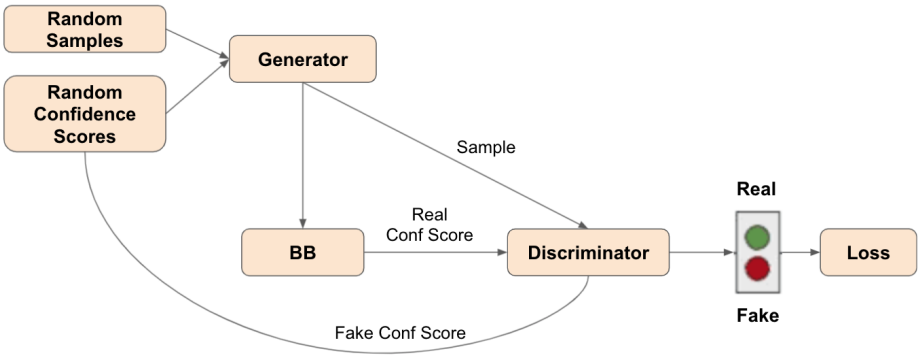
Samples that fooled the Discriminator:

Out of 100 generated samples, 43 fooled the Discriminator, while 57 did not.



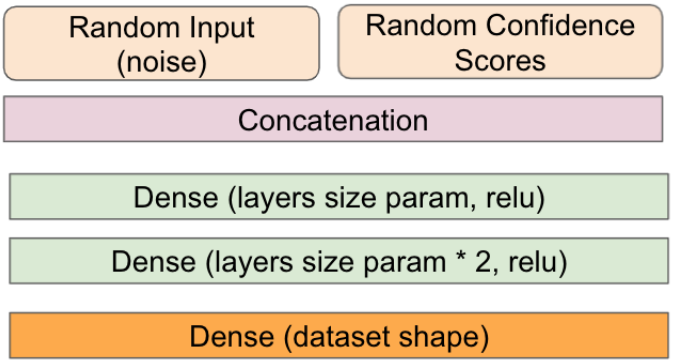


Part 2 – Generative model for sample generation

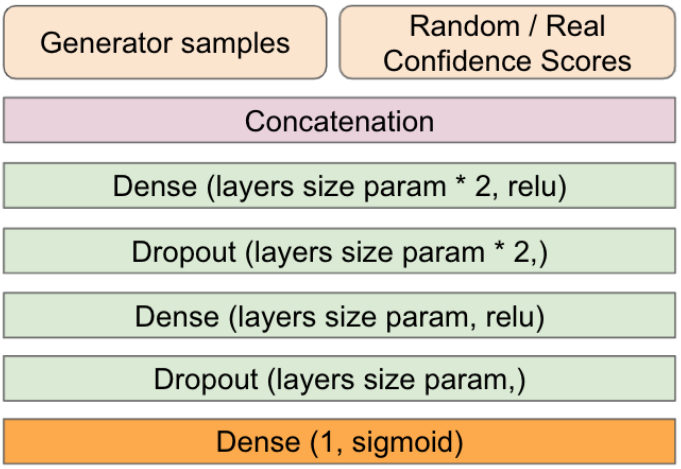


The architecture of the GAN:

The architecture of the Generator:



The architecture of the Discriminator:



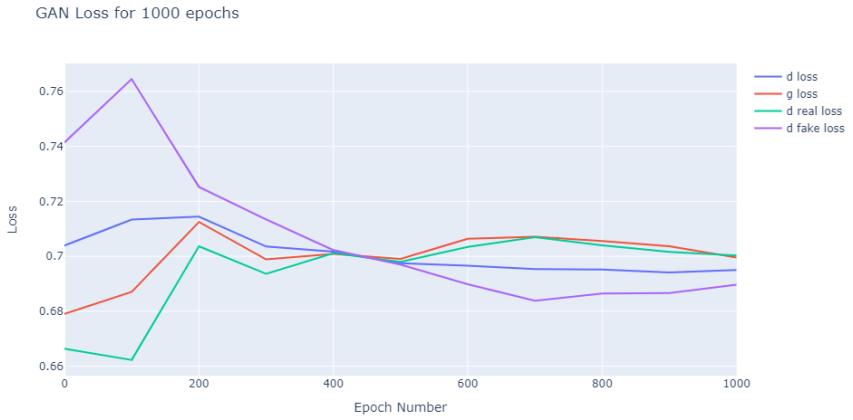
Results on Datasets - part 2:

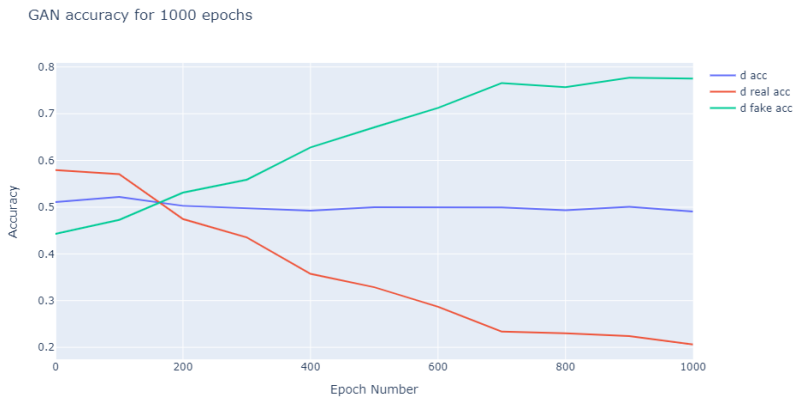
3. **Diabetes Dataset:**

Hyper parameters:

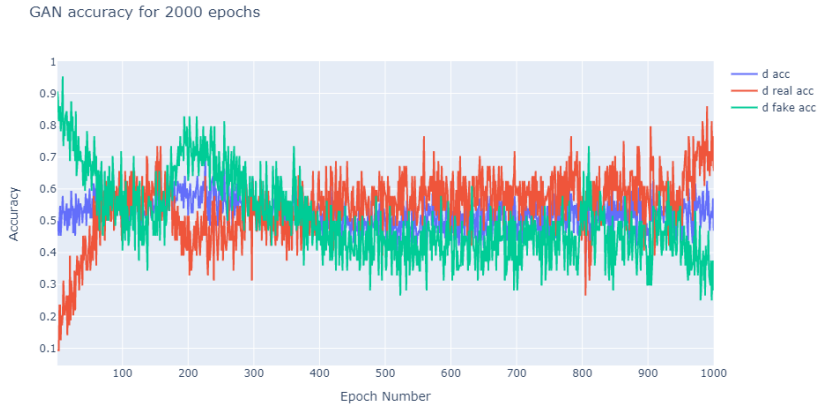
Parameter description	**Parameter value**
batch size	64
Number of epochs	1000
Learning rate	5e-4
Noise dimension size	8
Number of units in layers factor	16

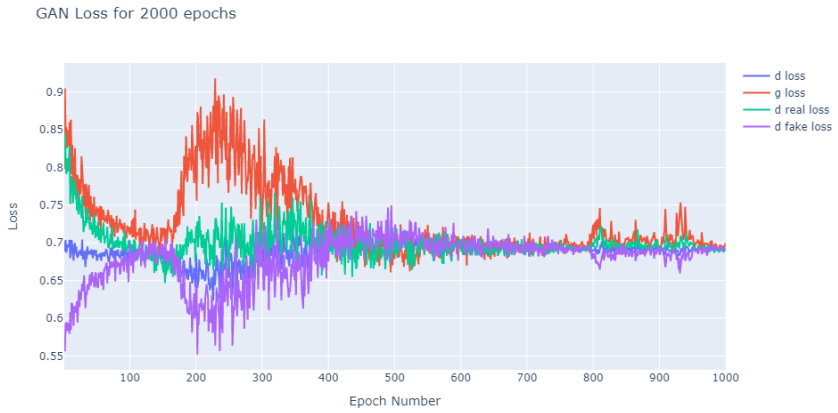
Average statistics per 100 epochs:





Raw statistics:

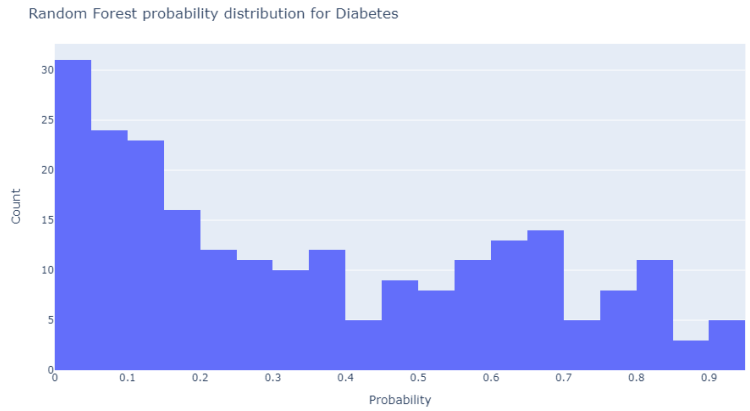




The GAN converged at epoch 1000.

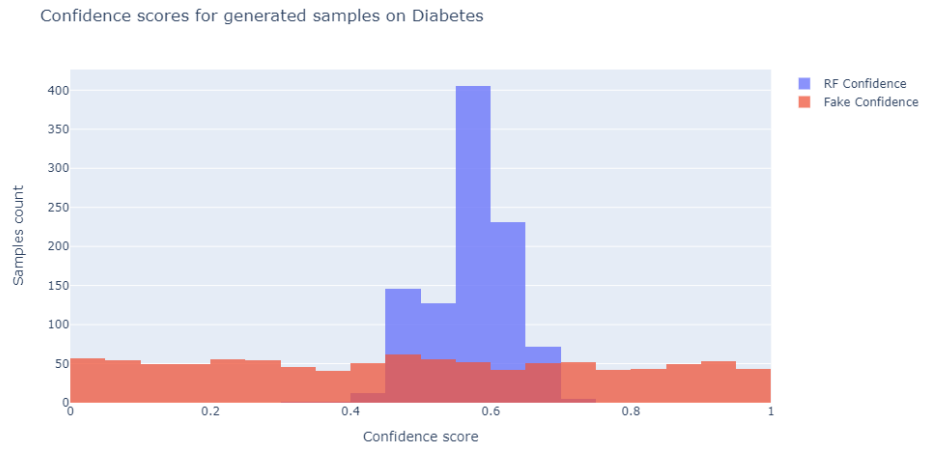
<u>The RandomForest classifier's performance:</u>

a. The classifier accuracy on test set (30%): 0.78
   Confidence score (Probability) distribution:
   Min: 0.004, Max: 0.942, Mean: 0.354

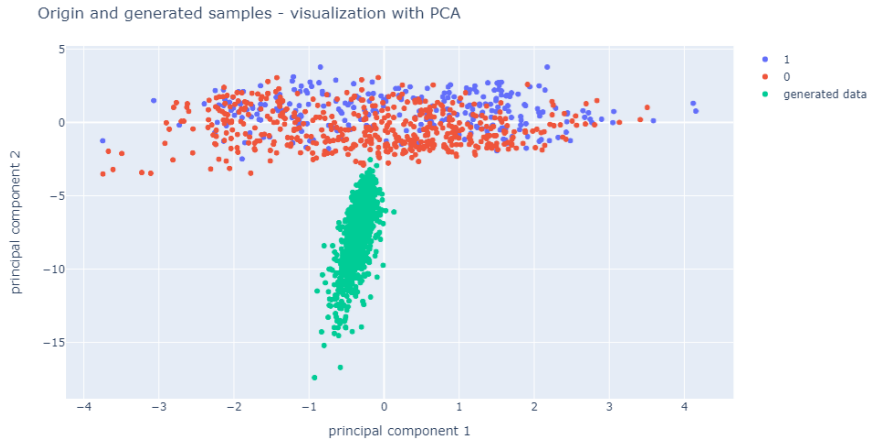


b. For generated samples (1000 samples):
   Confidence score (Probability) distribution:

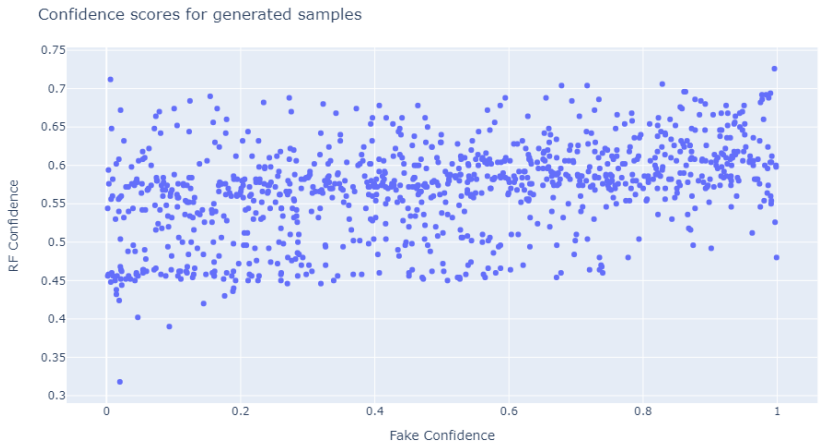
Fake- Min: 0, Max: 0.998, Mean: 0.487
RF- Min: 0.318, Max: 0.726, Mean: 0.568



It seems that the generator is generating samples that succeed to confuse the RF classifier, most of the samples receive ~0.5 confidence score.
We visualize both the generated samples and the origin data (using PCA dimension reduction), we can see that there is similarity between the generated data and the origin data (for both classes).



Correlation between RF confidence and Fake confidence: 0.421

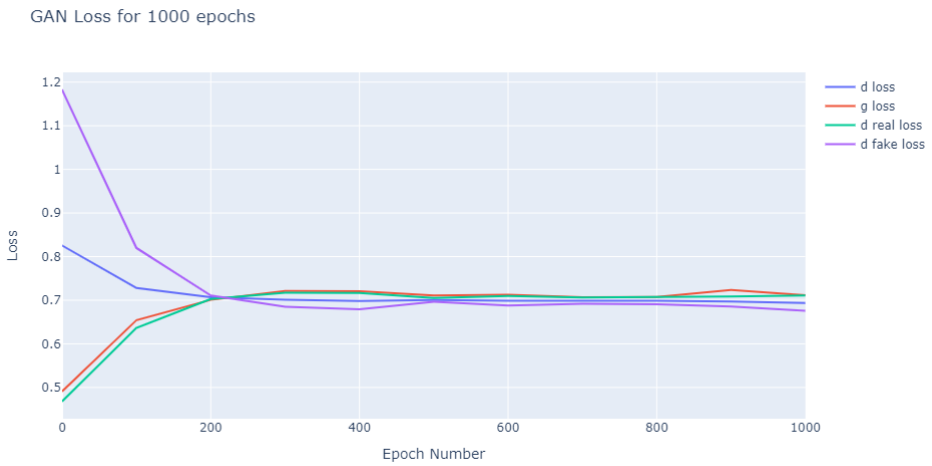


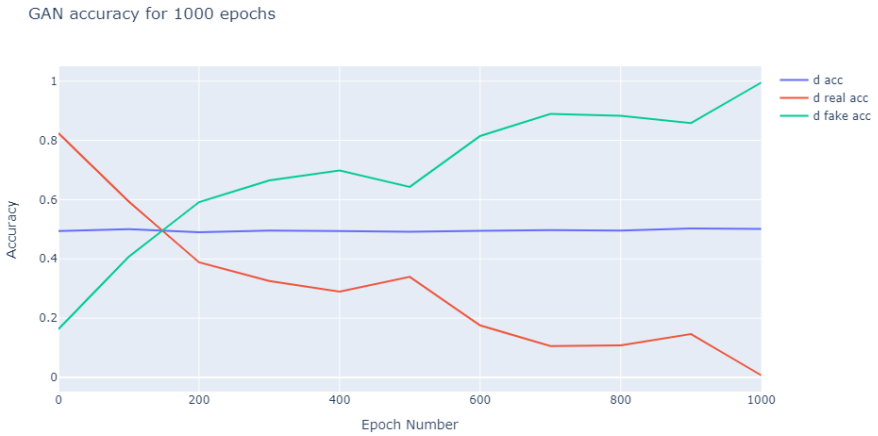
4. German credit Dataset:

Hyper parameters:

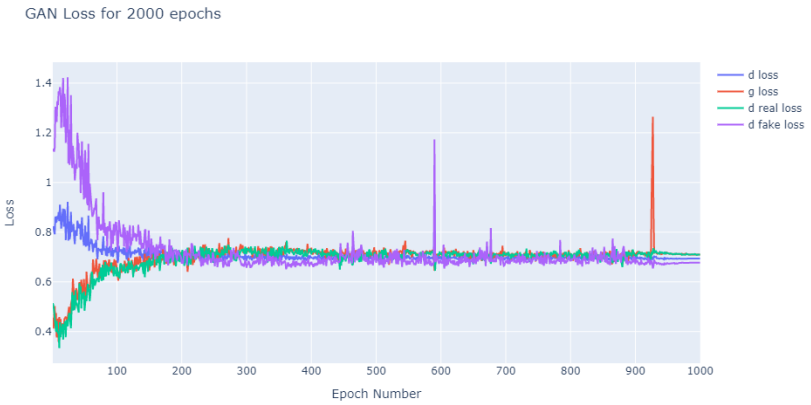
Parameter description	**Parameter value**
batch size	64
Number of epochs	1000
Learning rate	1e-3
Noise dimension size	48
Number of units in layers factor	20

Average statistics per 100 epochs:





Raw statistics:

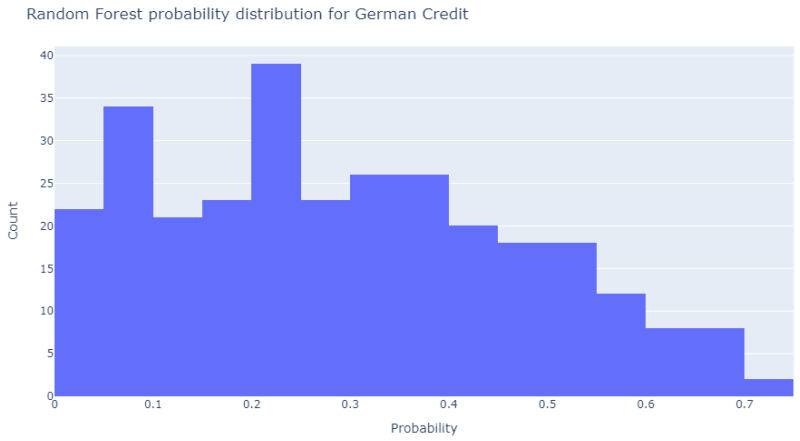


The GAN converged at epoch 1000.

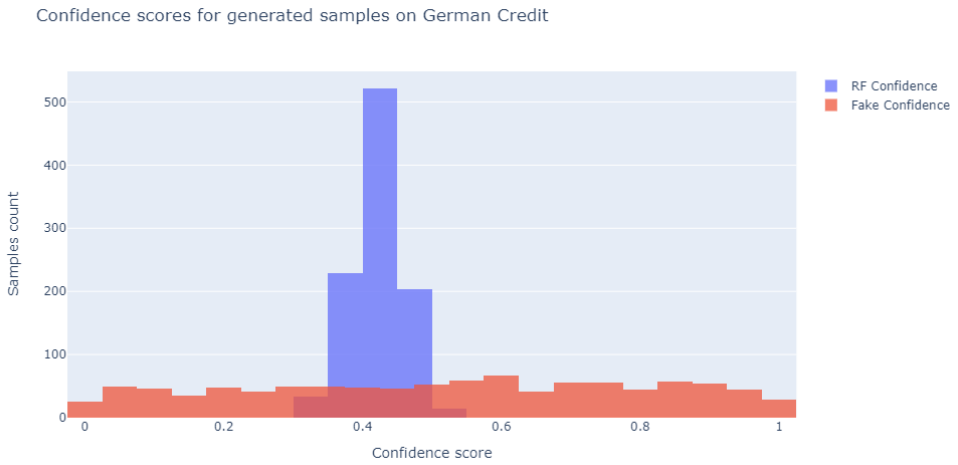
<u>The RandomForest classifier's performance:</u>

c. The classifier accuracy on test set (30%): 0.73
   Confidence score (Probability) distribution:

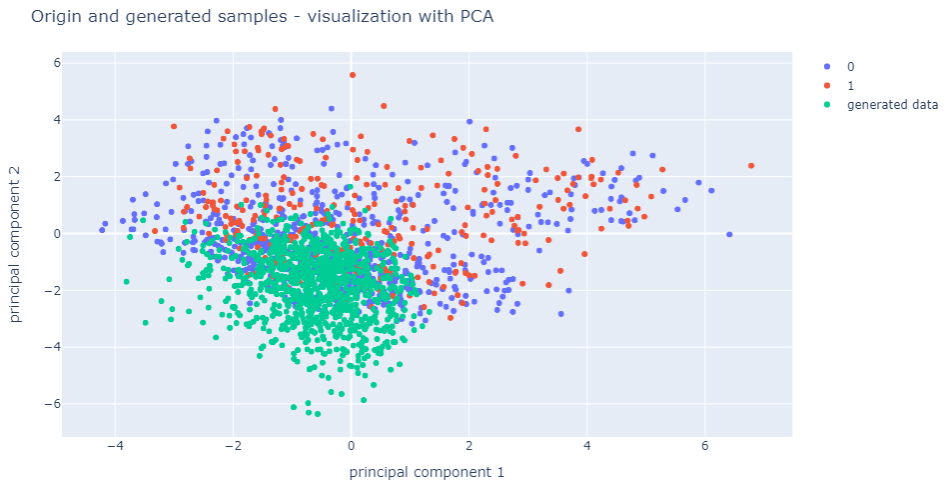
Min: 0.014, Max: 0.742, Mean: 0.294



d. For generated samples (1000 samples):
Confidence score (Probability) distribution:
Fake- Min: 0, Max: 0.997, Mean: 0.516
RF- Min: 0.31, Max: 0.518, Mean: 0.418



It seems that the generator is generating samples that are more biased toward the 0 class, the RF confidence score centers around ~0.4 confidence score.
We visualize both the generated samples and the origin data (using PCA dimension reduction), we can see that there is more similarity between the generated data and the 0 class in the origin data. We can see that the generator suffers from a Mode collapse issue, though it still succeeds in generating samples that are similar to class 1 as well.



Correlation between RF confidence and Fake confidence: -0.041