UCLA Samueli School of Engineering

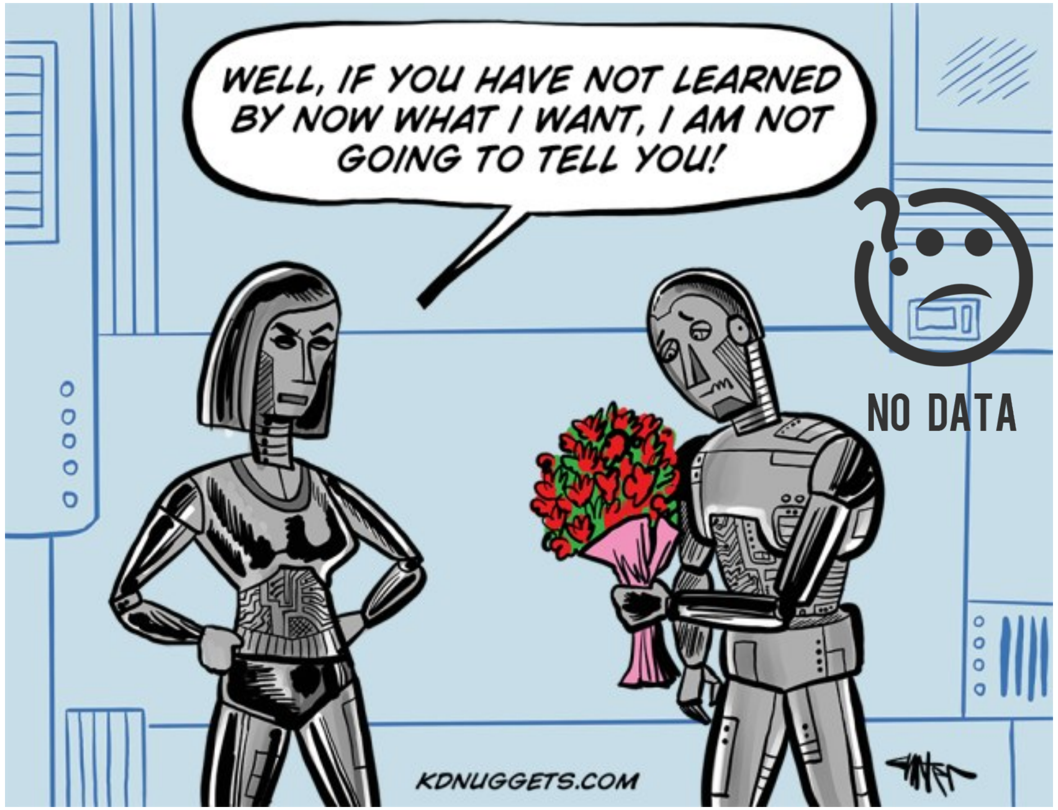
ECE 209AS Fall 2020 Bake-off 2 Final Presentation, 12/18/20

GUI-GAN: Towards an interactive graphical framework for privacy-preserving artificial data synthesis and imputation using generative adversarial networks.

Viacheslav Inderiakin and **Swapnil Sayan Saha**
Dept. of ECE, UCLA

Problem Statement

Hurdles in deploying AI-enabled interactive systems:

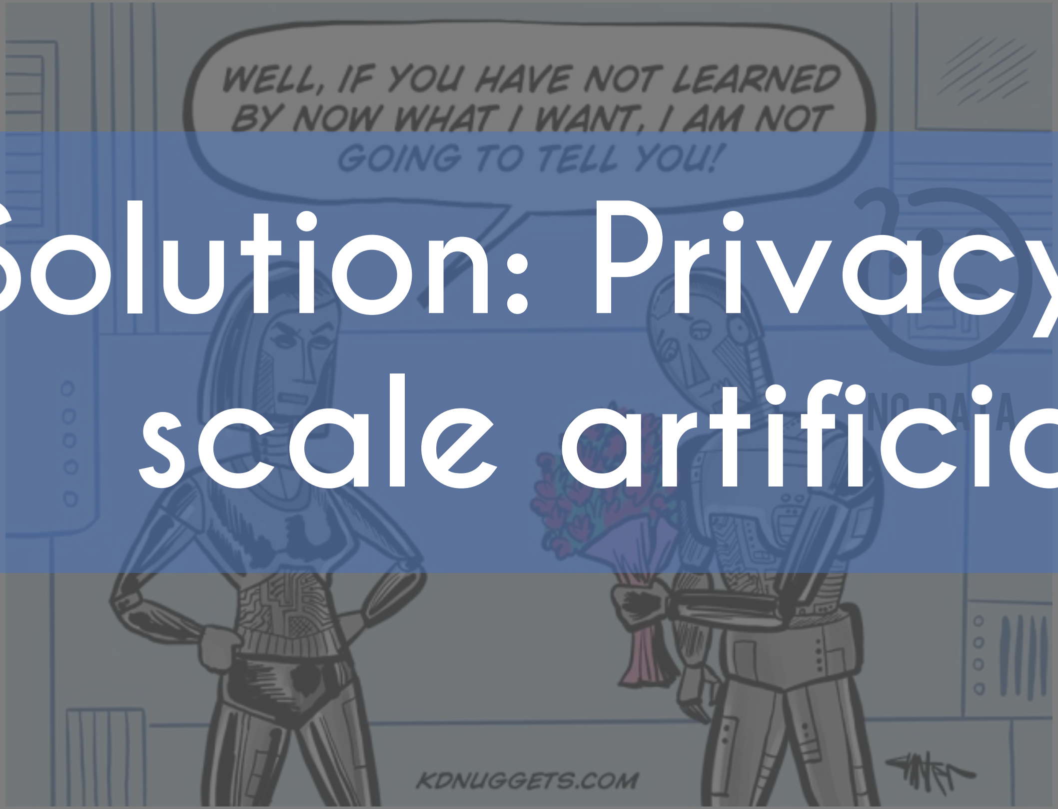


Lack of Data

Data Privacy

Problem Statement

Hurdles in deploying AI-enabled interactive systems:

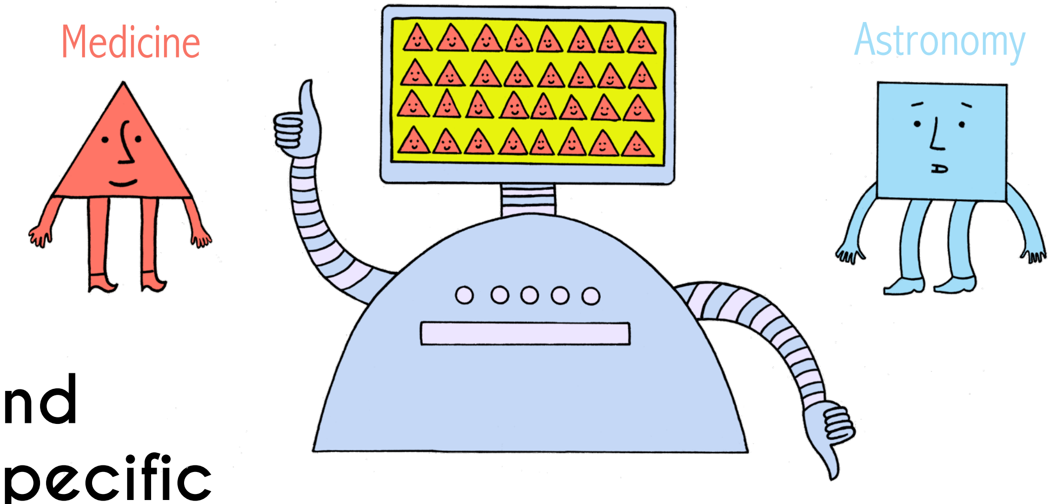


Lack of Data

Data Privacy

Solution: Privacy preserving large-scale artificial data synthesis

Existing Methods



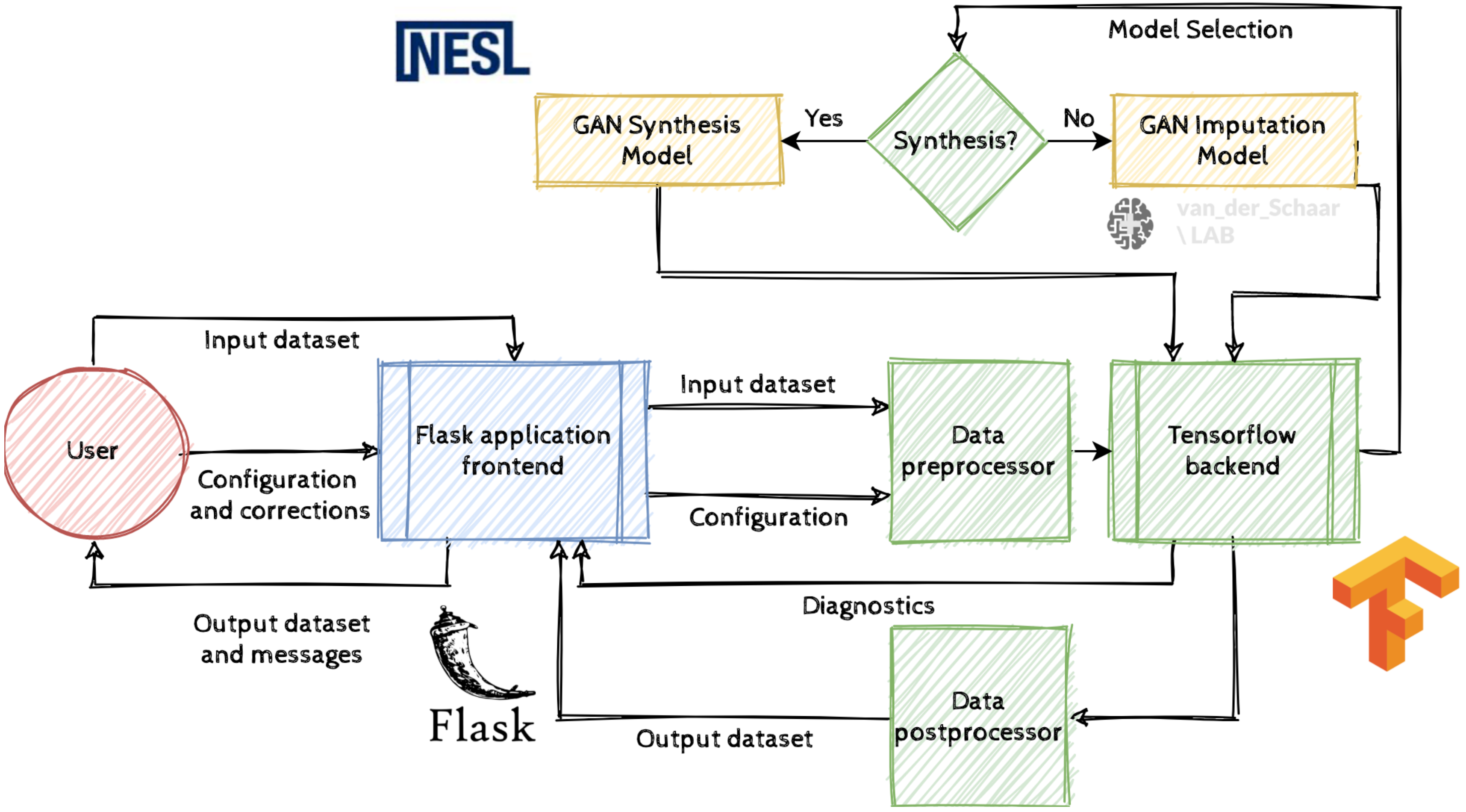
Domain and application-specific

Challenges in deploying existing artificial data synthesizers

Lack of interactivity and control

Computational and domain expertise required

Proposed Solution



GUI-GAN: A highly generalizable and AI-enabled synthetic time-series processing framework

Generates privacy preserving annotated multi-class datasets from small time-series datasets <u>in any domain</u>

<u>Collaborative and controllable</u>: allows user to make graph-based and symbolic corrections to groups of generated datasets

<u>Aimed for non-experts</u>: assumes zero machine-learning and coding expertise; runs on any generic computing device

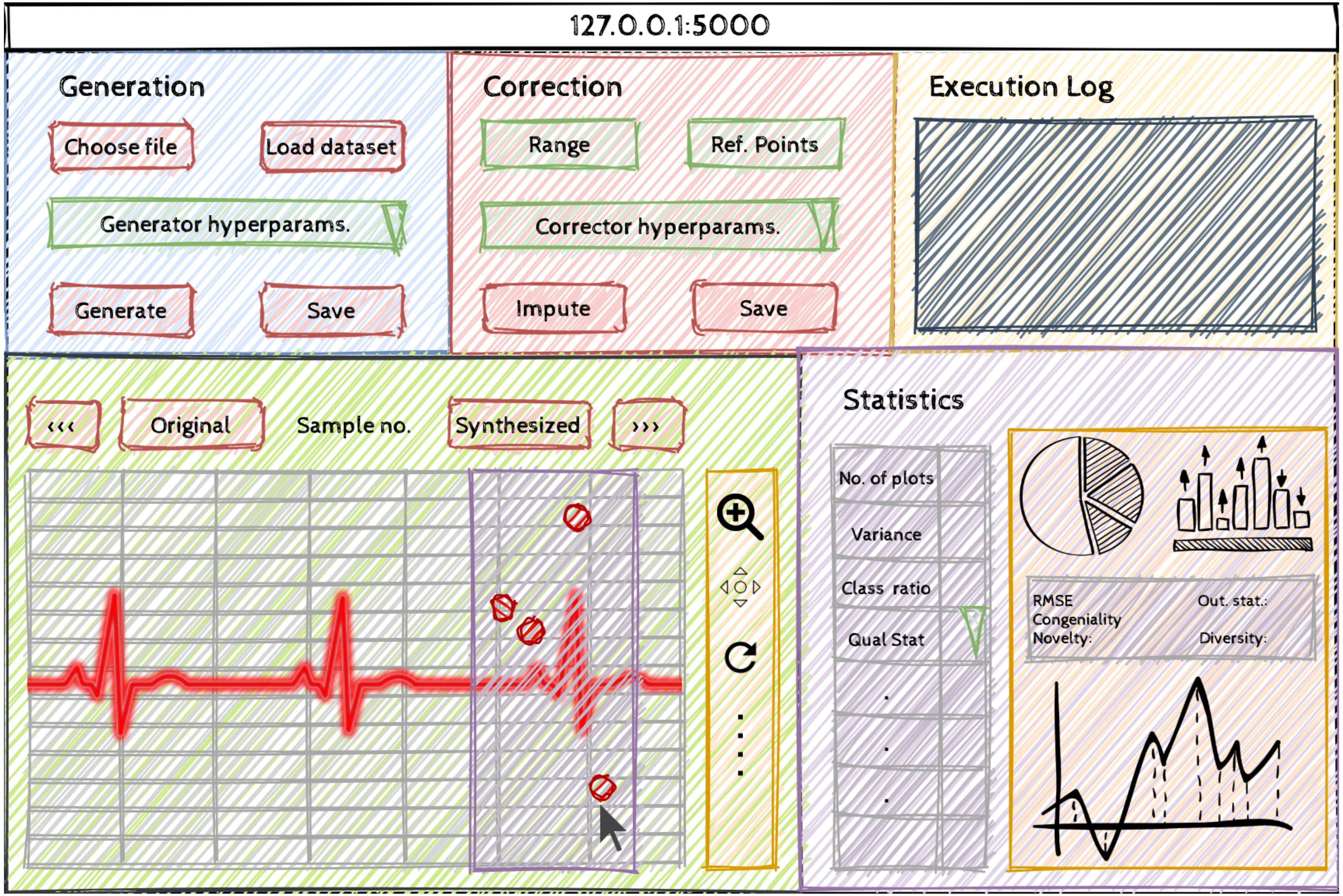
Challenges

- Providing a quick and responsive GUI for communicating with the AI during correction; no such interface exists that can:
  - provide sufficient tools to correct the plots in real-time, "on the fly;"
  - support integration with general-purpose GUI libraries

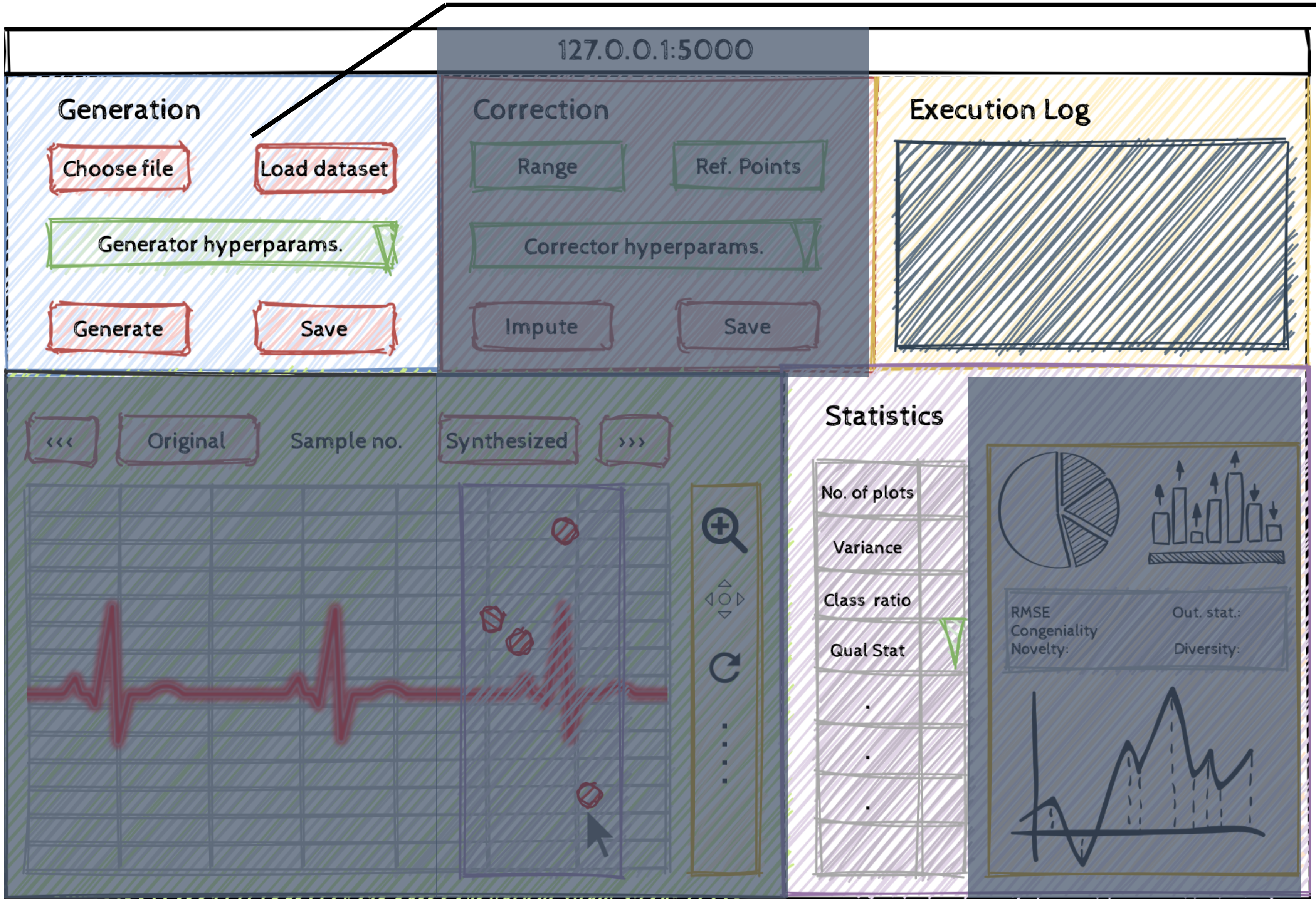
- Making sure the generated dataset is meaningful and useable by the end-user (controlling variability)
  - As Patrick's team mentioned, GANs can often produce garbage
  - It's important to incorporate the notion of condition in the GAN

- **Solutions:**
  - **Couple Bokeh, Flask python libraries and Java for designing web-application to meet the desired requirements for responsiveness.**
  - **Incorporate novelty and diversity losses in GAN, along with utility checks with tertiary AI, as well as comparing various distributions.**

Storyboard (Synthesis)



Storyboard (Synthesis)



Choose file to specify directory of small dataset as zip file

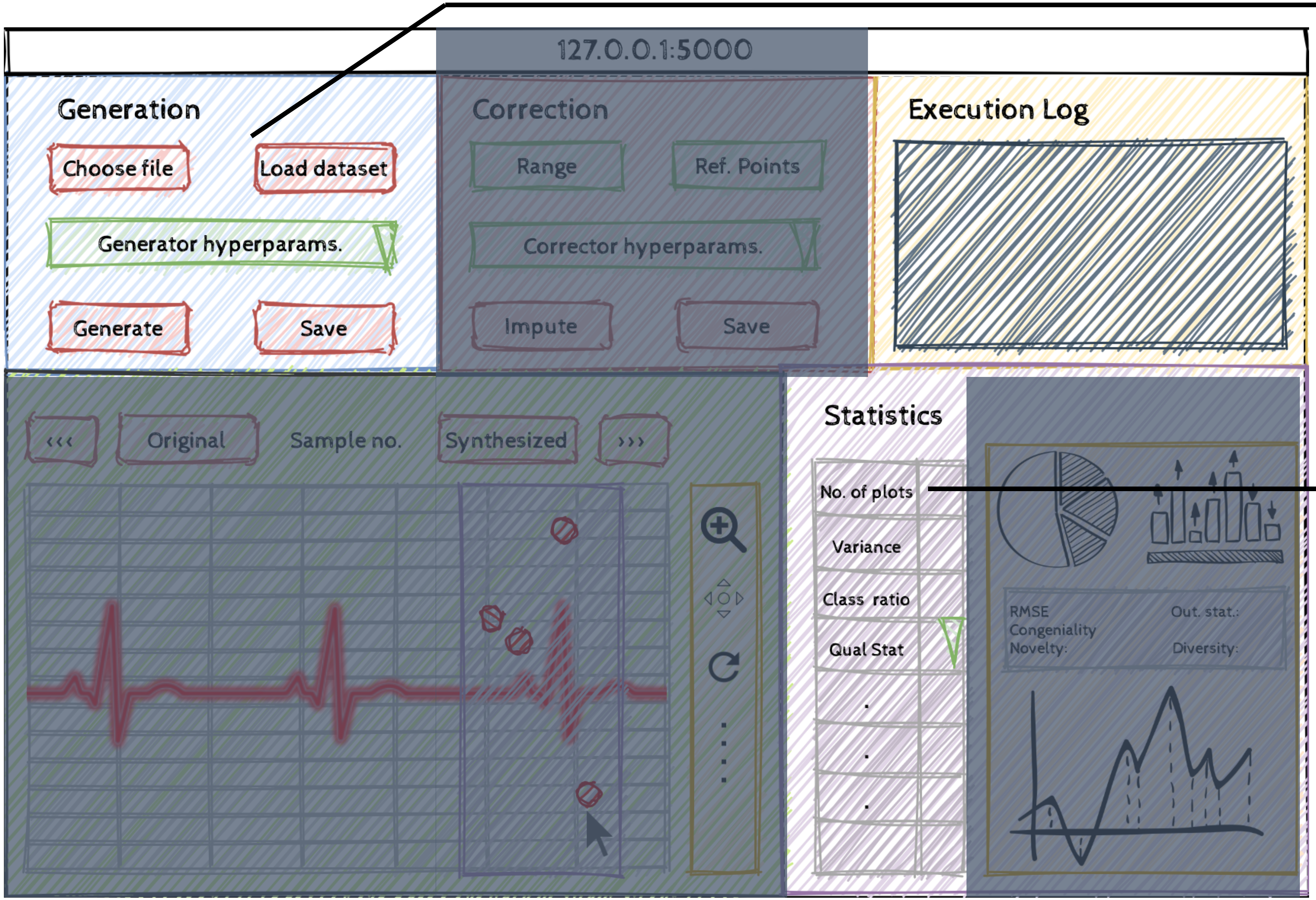
Click load dataset to load data into memory

Specify generator hyperparameters (listed in non-technical language with explanation)

Input coveted dataset statistics symbolically in the table

Click generate and wait for model to train and synthesize with training log shown in execution

Storyboard (Synthesis)



1

Choose file to specify directory of small dataset as zip file

Click load dataset to load data into memory

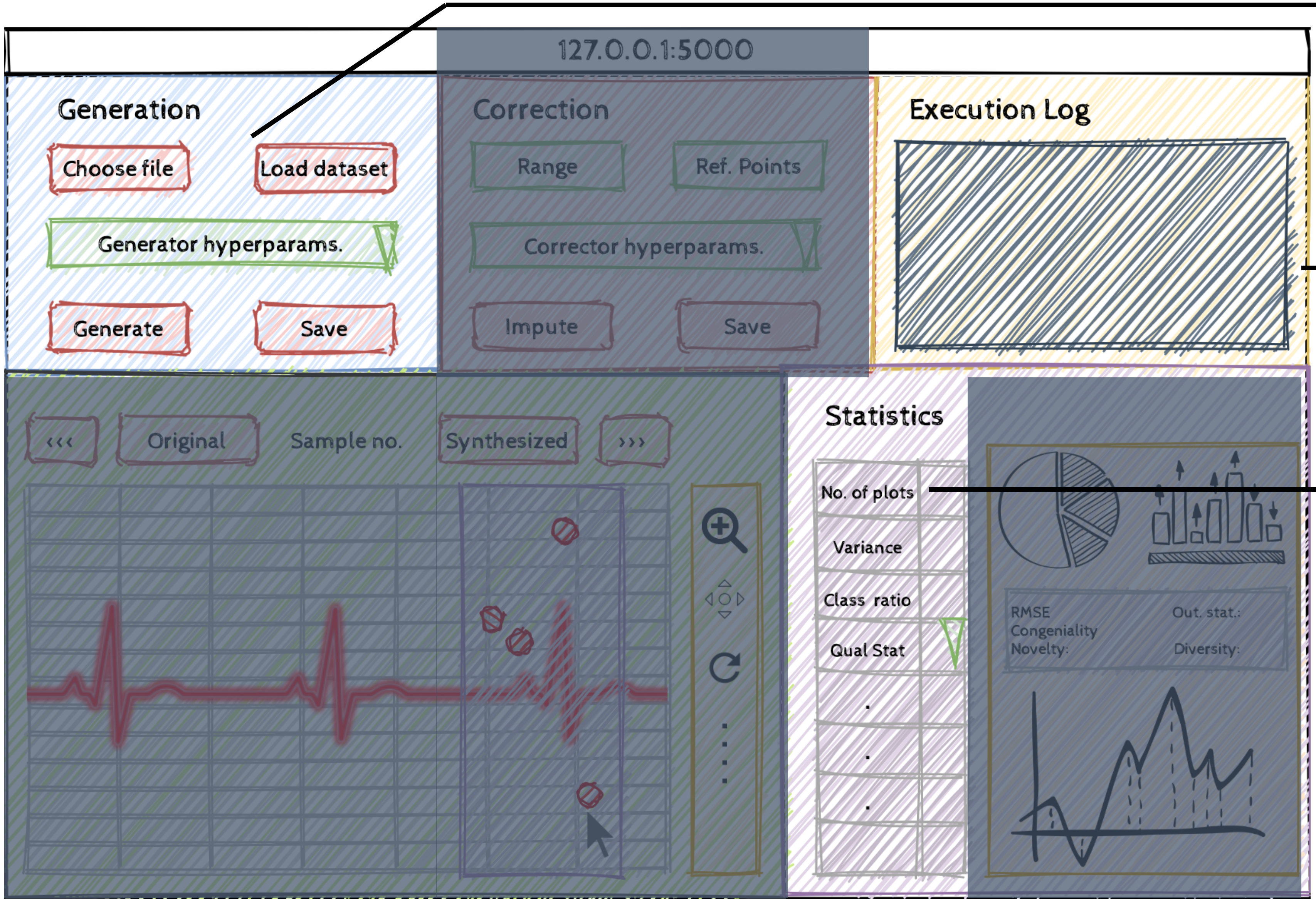
Specify generator hyperparameters (listed in non-technical language with explanation)

2

Input coveted dataset statistics symbolically in the table

Click generate and wait for model to train and synthesize with training log shown in execution

Storyboard (Synthesis)



1

Choose file to specify directory of small dataset as zip file

Click load dataset to load data into memory

Specify generator hyperparameters (listed in non-technical language with explanation)

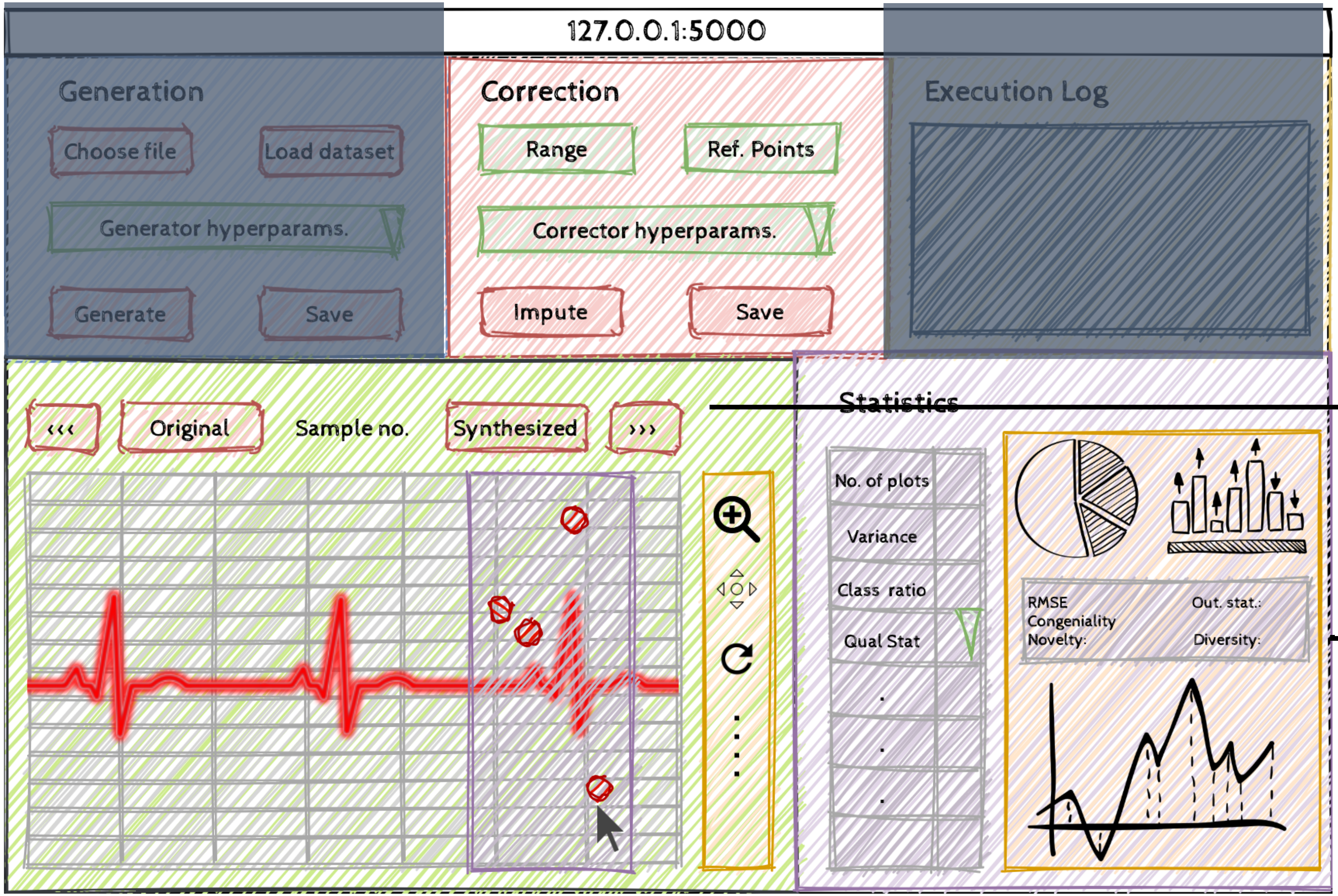
2

Input coveted dataset statistics symbolically in the table

3

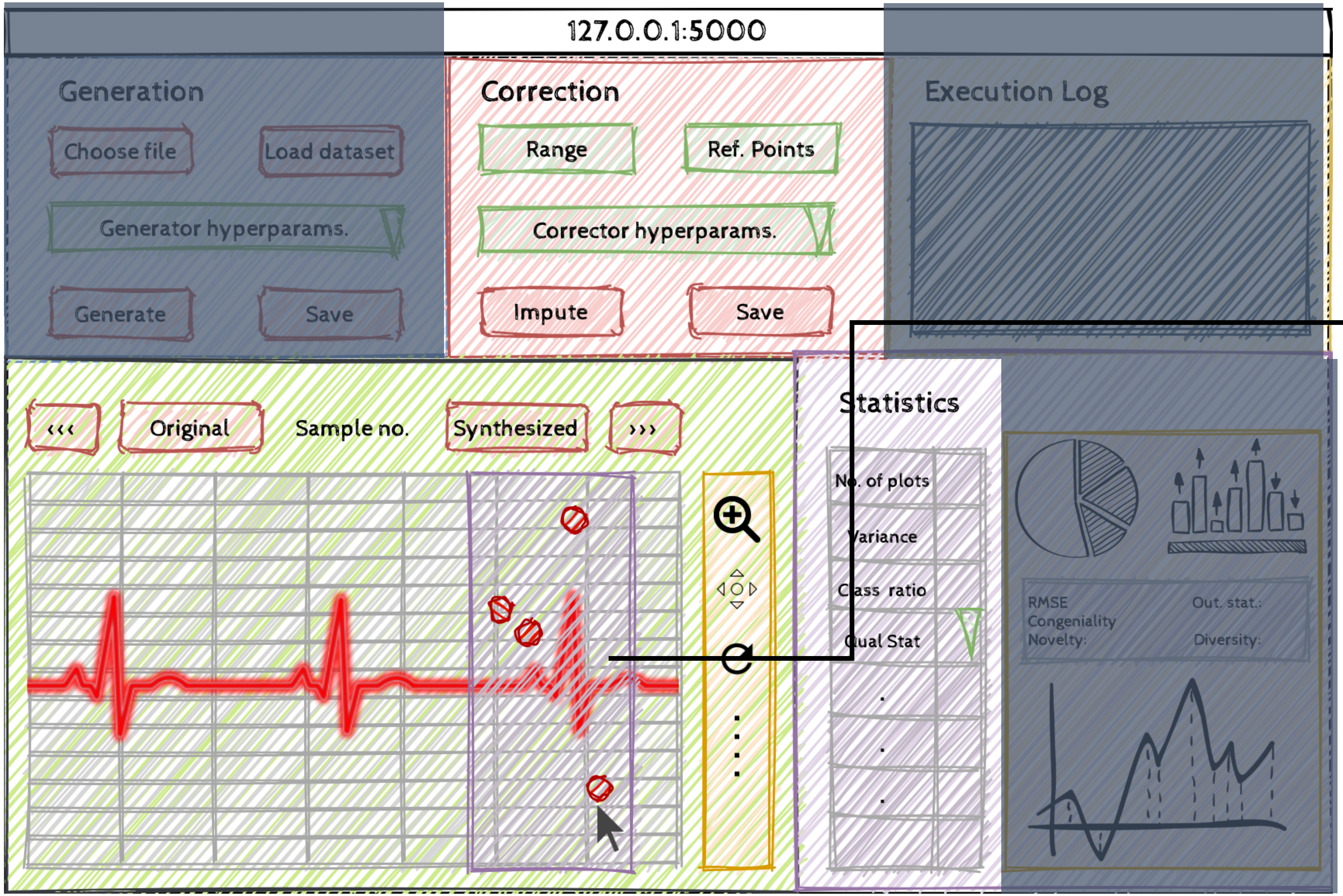
Click generate and wait for model to train and synthesize with training log shown in execution

Storyboard (Correction)



1. Check plots in the graphical window (use arrow keys to move between plots), check generated dataset statistical plots in statistics window
2. Specify correction by drawing bounding box and clicking guide points
3. Input imputation parameters
4. Input coveted dataset statistics in the table
5. Click impute and wait for model to train and synthesize with training log shown in execution

Storyboard (Correction)



Check plots in the graphical window (use arrow keys to move between plots), check generated dataset statistical plots in statistics window

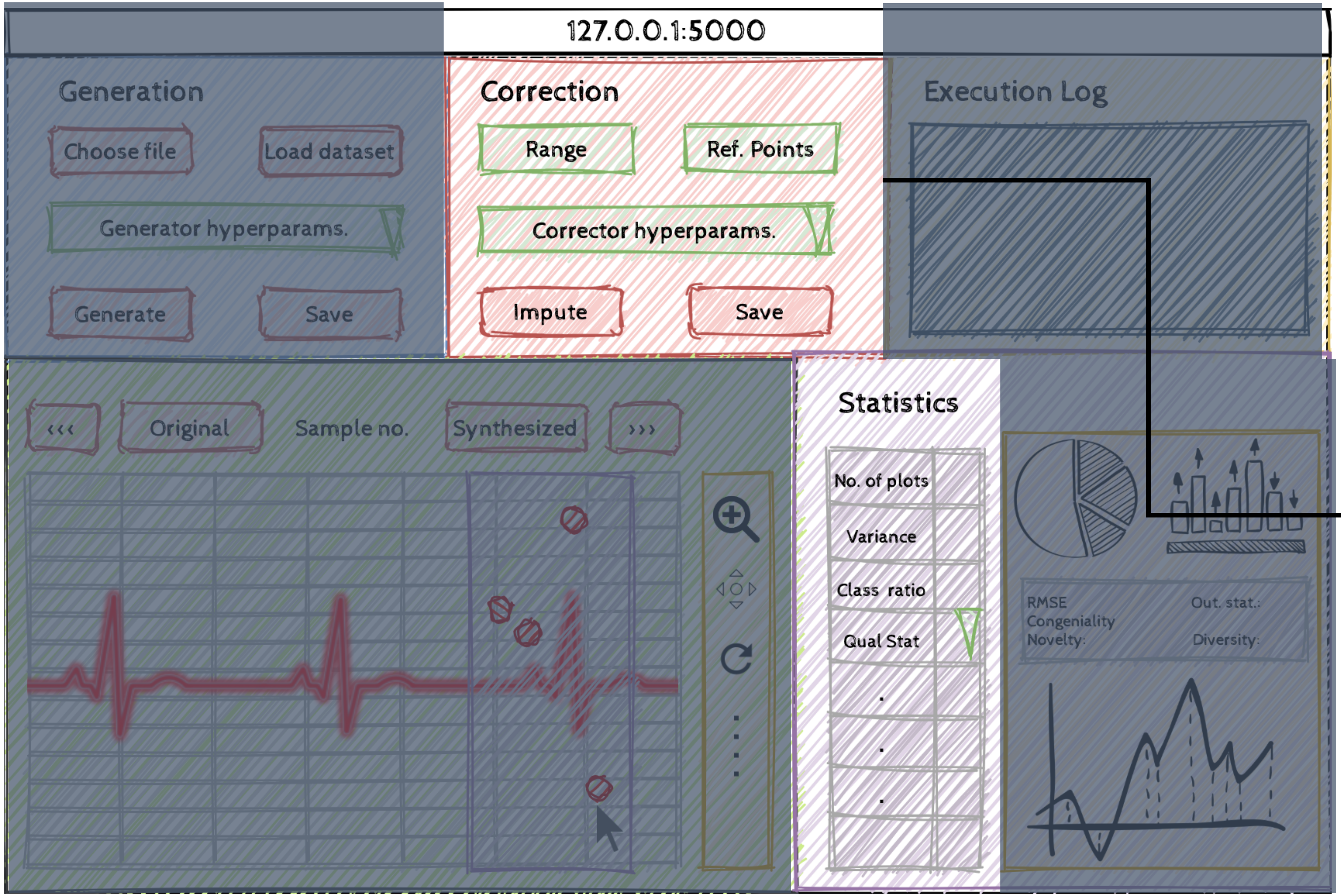
Specify correction by drawing bounding box and clicking guide points

Input imputation parameters

Input coveted dataset statistics in the table

Click impute and wait for model to train and synthesize with training log shown in execution

Storyboard (Correction)



Check plots in the graphical window (use arrow keys to move between plots), check generated dataset statistical plots in statistics window

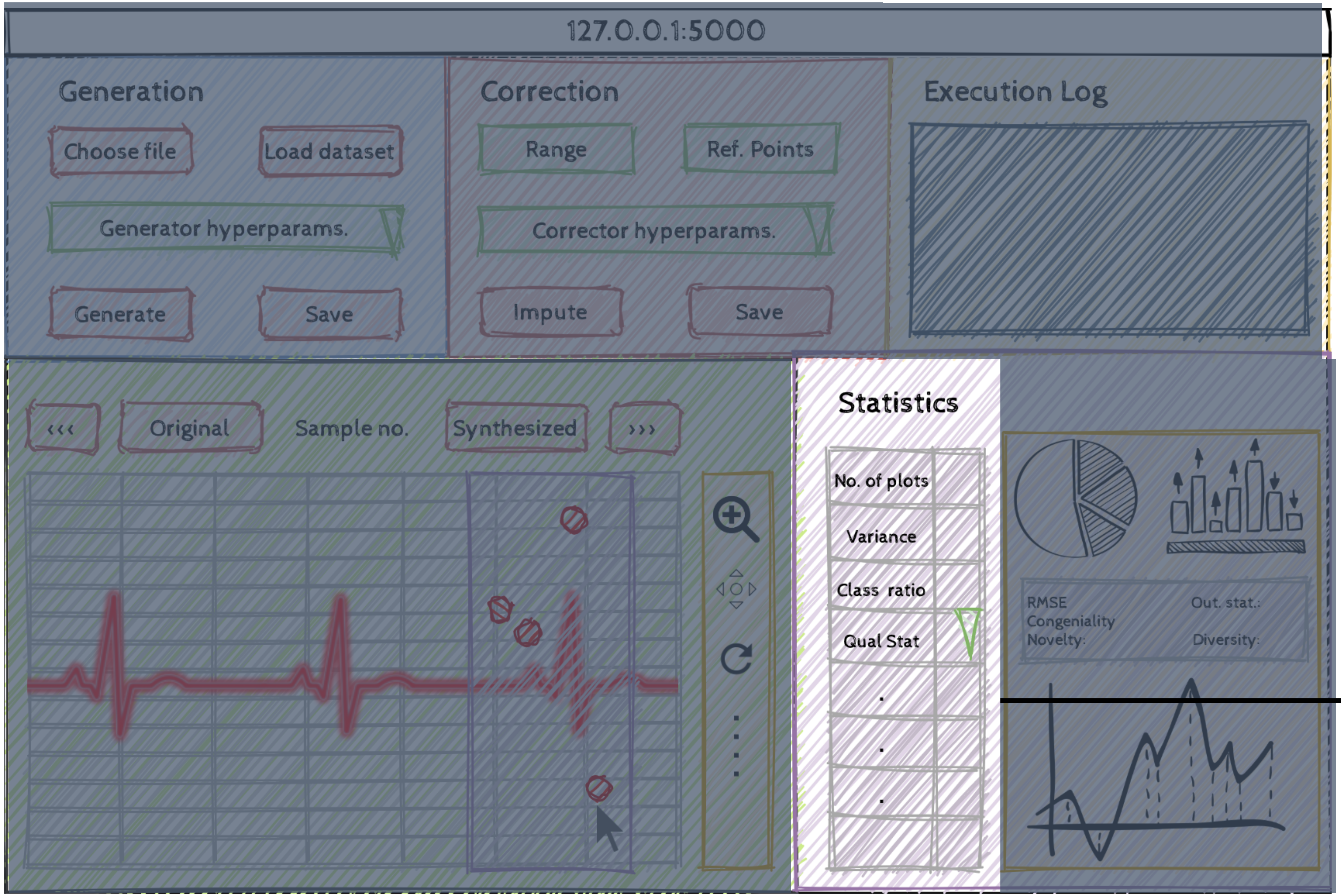
Specify correction by drawing bounding box and clicking guide points

Input imputation parameters

Input coveted dataset statistics in the table

Click impute and wait for model to train and synthesize with training log shown in execution

Storyboard (Correction)



Check plots in the graphical window (use arrow keys to move between plots), check generated dataset statistical plots in statistics window

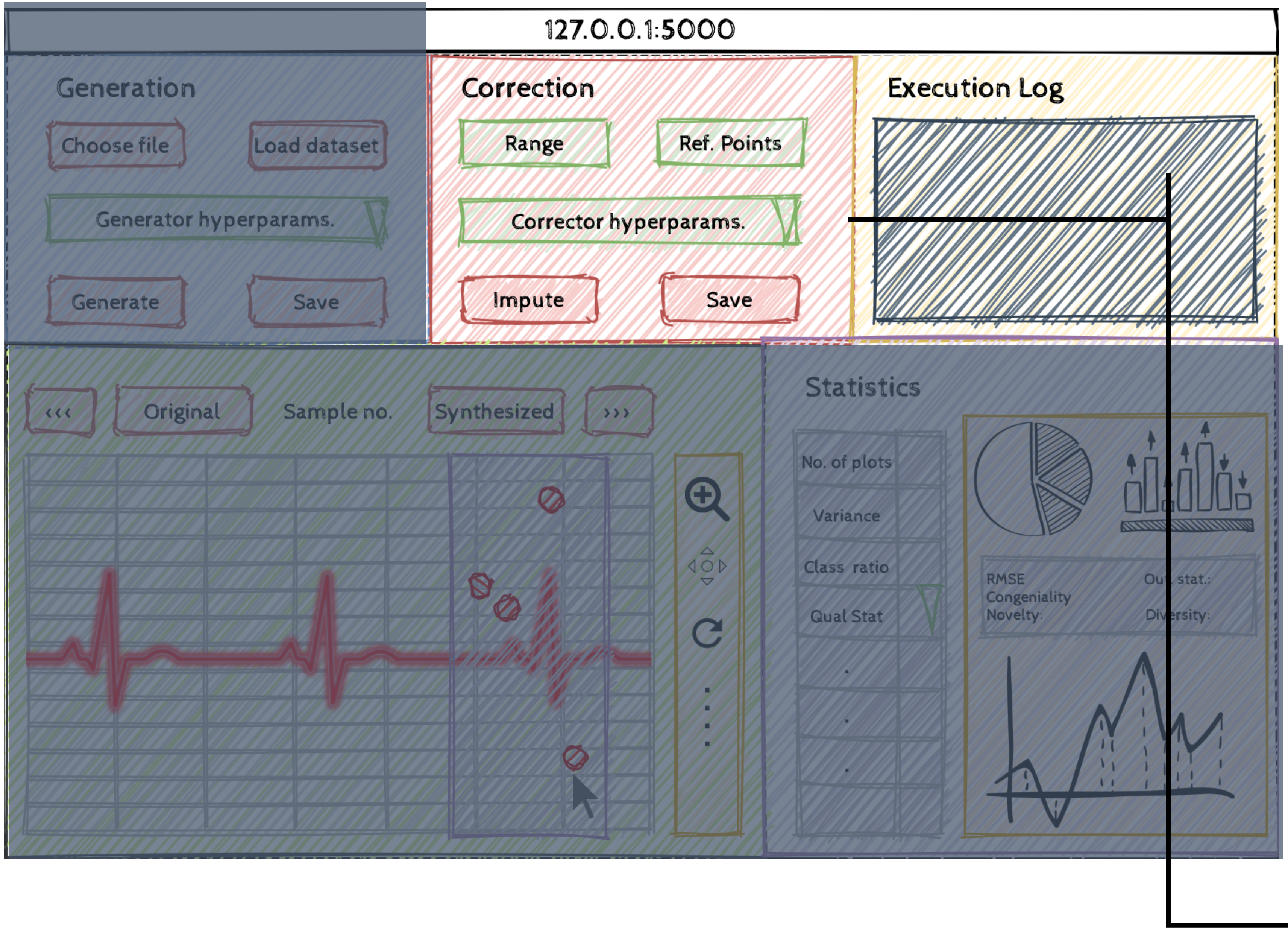
Specify correction by drawing bounding box and clicking guide points

Input imputation parameters

Input coveted dataset statistics in the table

Click impute and wait for model to train and synthesize with training log shown in execution

Storyboard (Correction)



Check plots in the graphical window (use arrow keys to move between plots), check generated dataset statistical plots in statistics window

Specify correction by drawing bounding box and clicking guide points

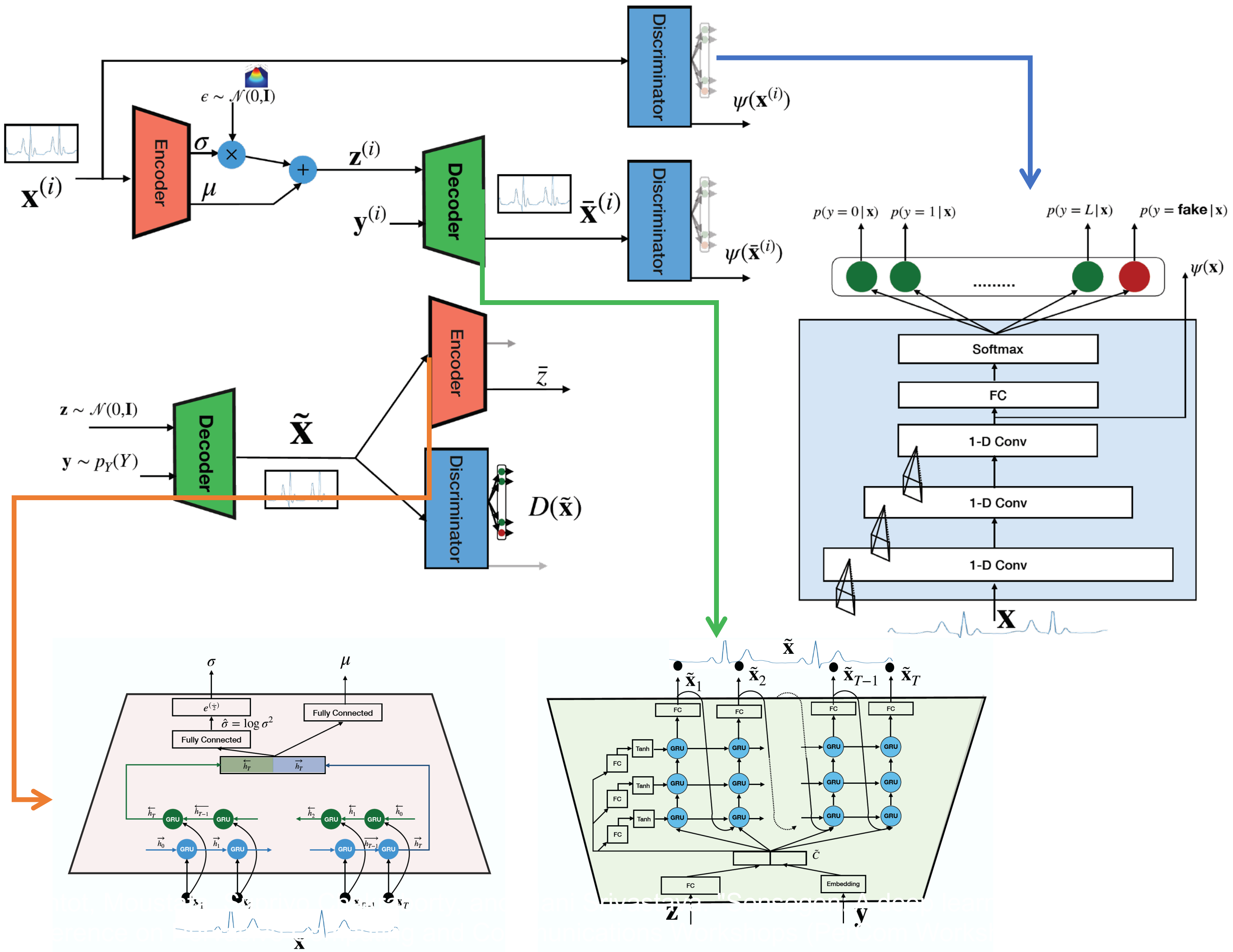
Input imputation parameters

Input coveted dataset statistics in the table

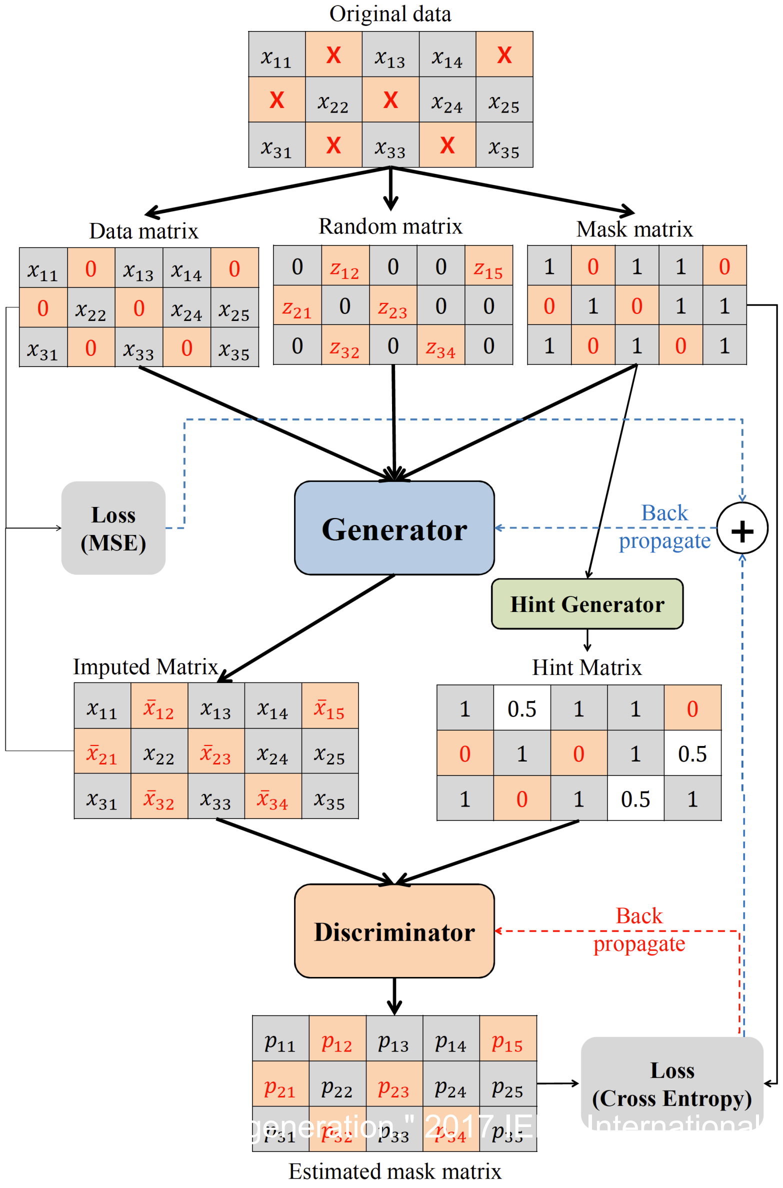
Click impute and wait for model to train and synthesize with training log shown in execution

GAN-framework

Dataset synthesizer (PhysioGAN)



Dataset corrector (GAIN)



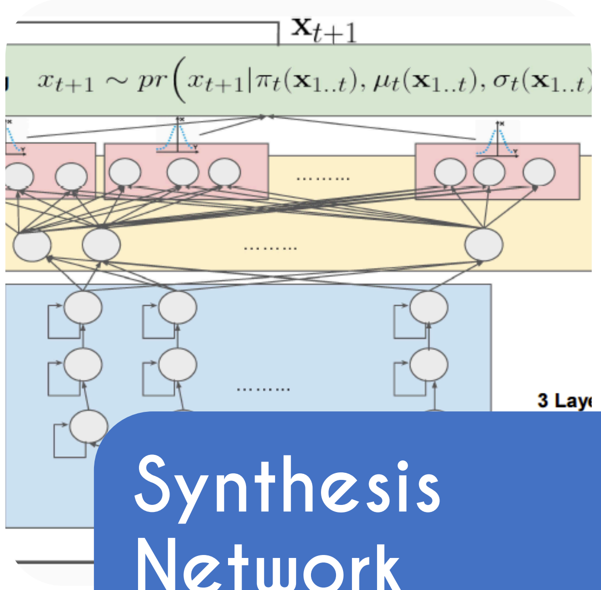
[1]. Alzantot, Moustafa Farid Taha Mohammed. “Secure and Private Machine Learning for Smart Devices”. Ph.D. Diss. UCLA, 2019.

[2]. Yoon, Jinsung, James Jordon, and Mihaela van der Schaar. " GAIN: Missing Data Imputation using Generative Adversarial Nets. " International Conference on Machine Learning (ICML). 2018.

Evaluation Metrics

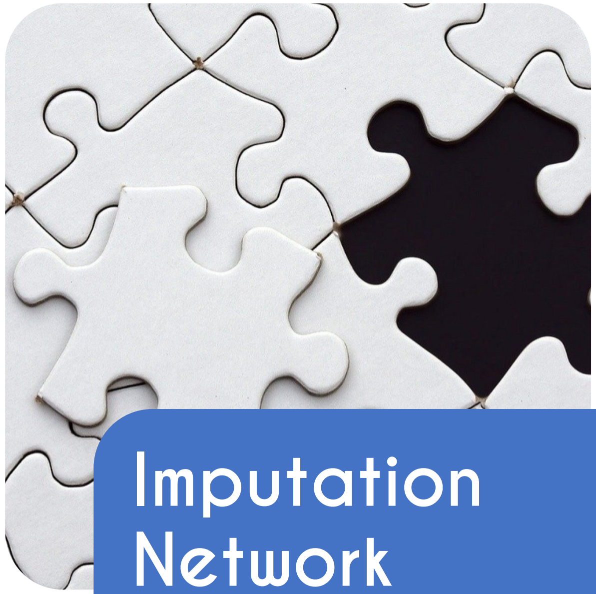
Privacy Preservation

- Synthesis GAN discriminator misclassification rate



Synthesis Network

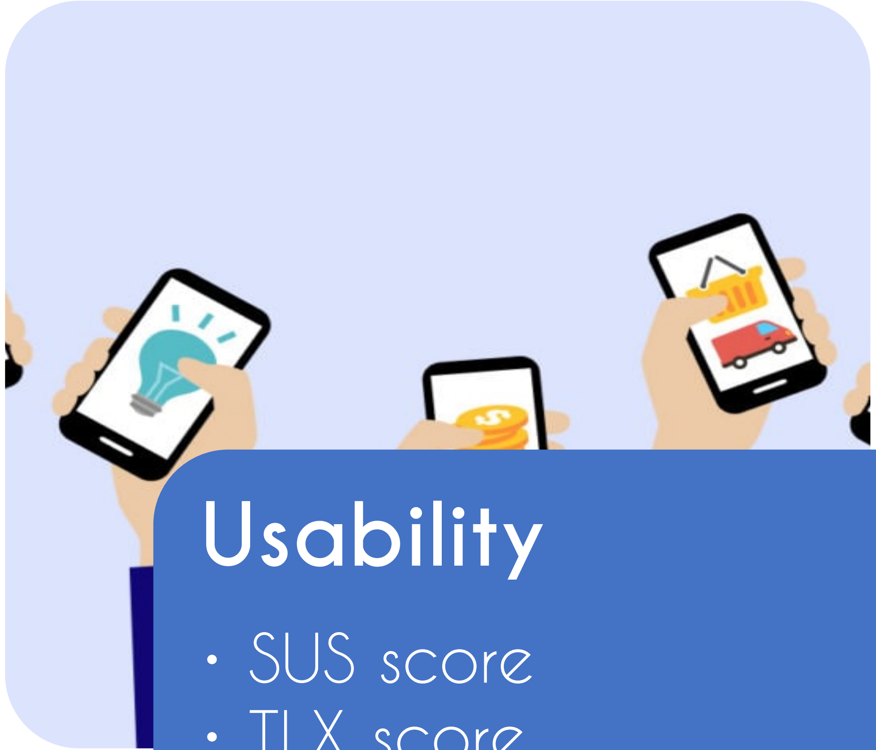
- RMSE of output dataset statistics with input dataset statistics
- Discriminative and predictive losses



Imputation Network

- RMSE and AUROC with varying missing rates
- Congeniality of data imputation network

User Satisfaction Metrics



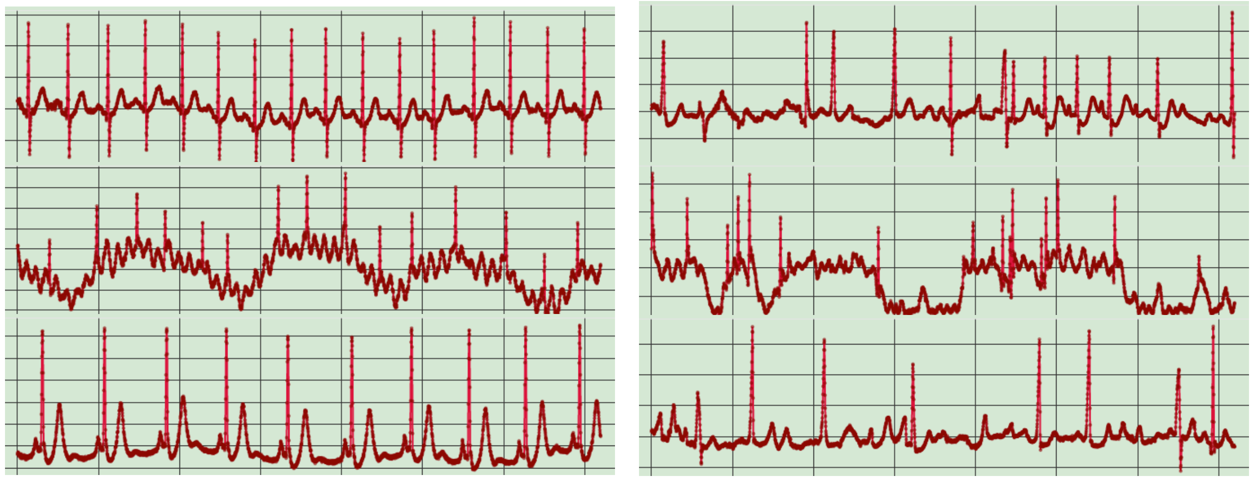
Usability

- SUS score
- TLX score
- General feedback and suggestions

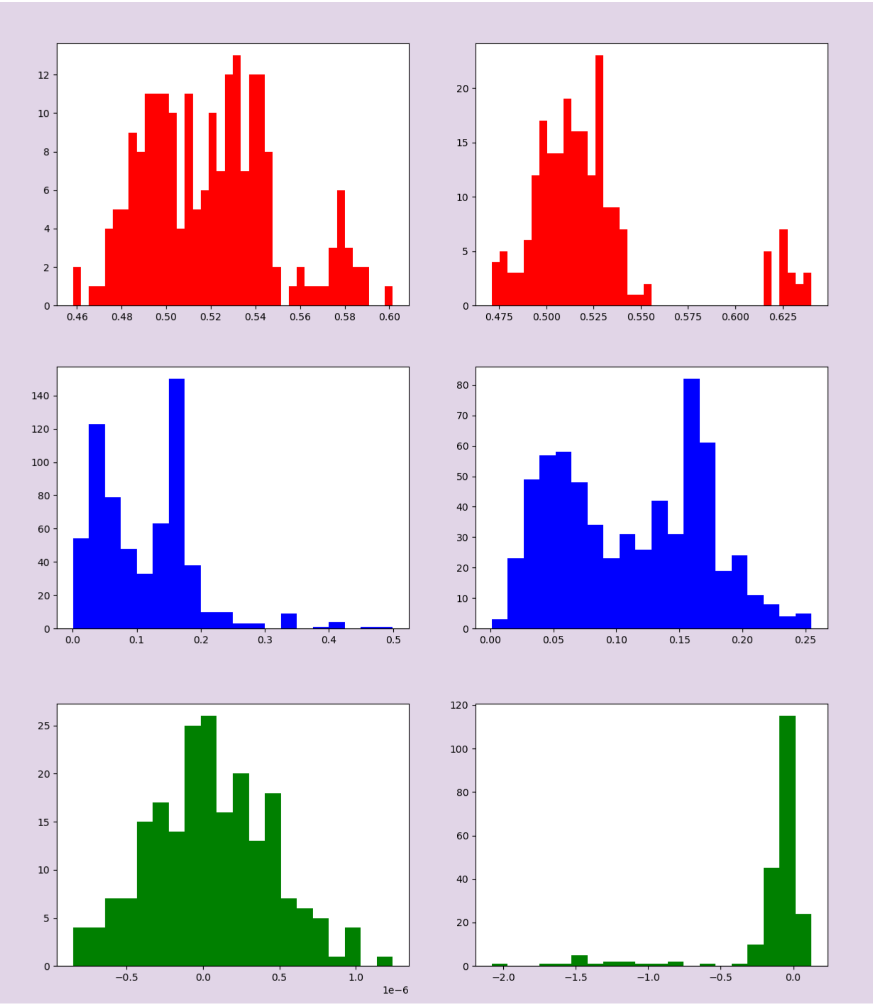
Controllability and collaboration

- Novelty and diversity of dataset w.r.t. user parameters
- Utility with tertiary model w.r.t. user parameters
- General feedback

Evaluation and Cont./Coll. Metrics



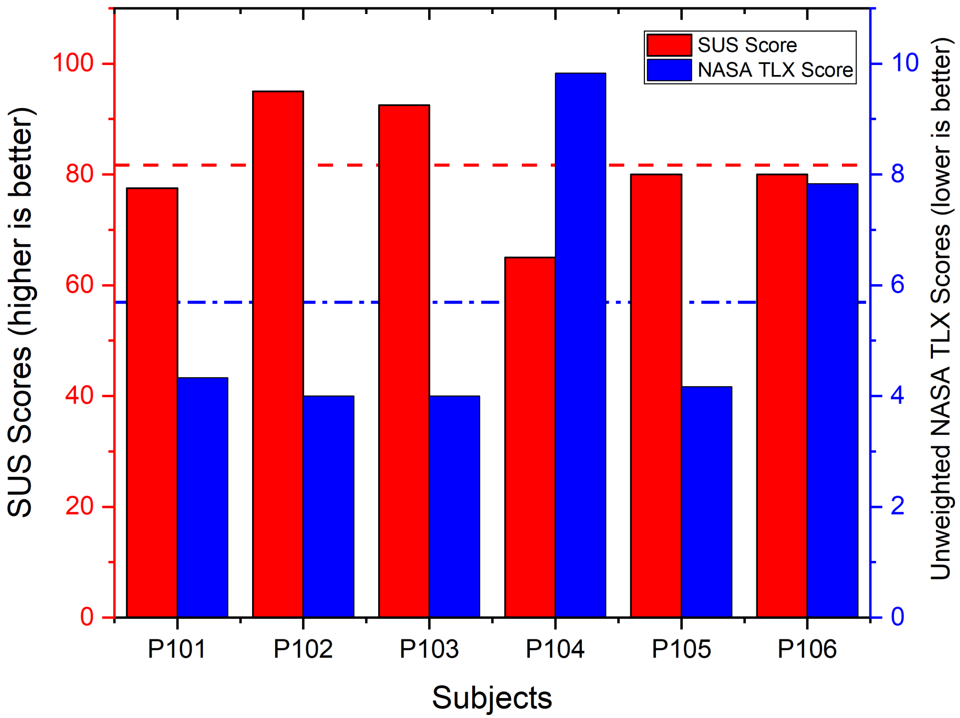
(Left): Sample ECG plots from real dataset, (Right) Sample ECG plots from synthetic datasets

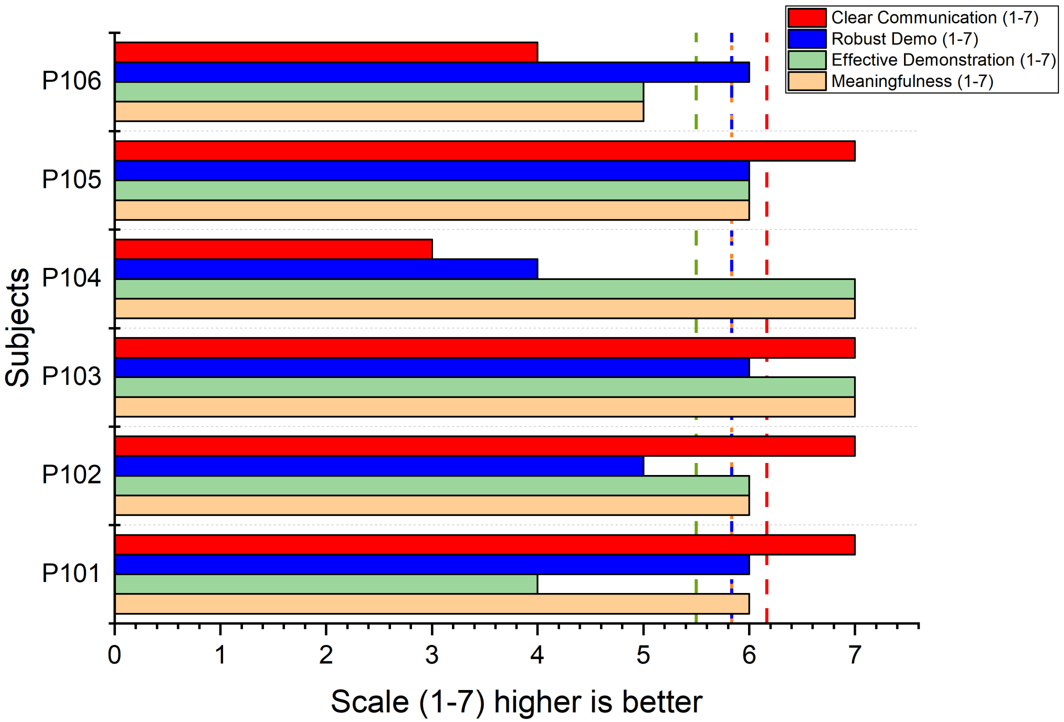


Example dataset distributions for ECG dataset. Red: Diversity distribution of original dataset vs. generated dataset. Blue: Novelty distribution of original dataset vs. generated dataset. Green: Mean distribution of original dataset vs generated dataset. Div. and nov. dist. should be similar, while mean dist. should be slightly different for privacy preservation

- **Discriminator misclassification rate for ECG dataset:** ~50%
- **Mean GAN loss for ECG dataset:** -1.6581
- **RMSE of output dataset statistics with input dataset statistics for ECG dataset:** 0.93893
- **Global novelty score difference for ECG dataset:** 0.00125
- **Global diversity score difference for ECG dataset:** 0.00395
- **Utility** (tested with tertiary RNN on ECG dataset): 0.87 (vs. 0.96 on real world dataset)
- **Imputation network performance** (from paper):
  - **RMSE:** Spam: 0.0513, Credit: 0.1858 News: 0.1441
  - **AUROC:** Spam: 0.9529, Credit: 0.7527 News: 0.9711

User Study – SUS, TLX and Rubrics





- **Shapiro-Wilk Test**: Bias found in NASA TLX, “robustness of demo” and “communication clarity”
- **Usability grade [1]:** A (best possible), **Workload category [2]**: Low (best possible)
- **Average rubric scores** (out of 7):
    - Meaningfulness: 6.2
    - Effective Demonstration: 5.8
    - Robustness of Demo: 5.5
    - Communication Clarity: 5.8

[1]. Sauro, Jeff. "Measuring usability with the system usability scale (SUS)." (2011).
[2]. Prabaswari, Atyanti Dyah, Chancard Basumerda, and Bagus Wahyu Utomo. "The Mental Workload Analysis of Staff in Study Program of Private Educational Organization." IOP Conference Series: Materials Science and Engineering. Vol. 528. No. 1. IOP Publishing, 2019.

General Feedback

Easy and Natural	*"…clear, sensible workflow…" "…even a beginner can use it easily…"* *"…clear instructions; buttons similar to other apps and hence natural…."* *"…intuitive design…"* *"…provided the context to the client, the interface is easy and natural…"*
Useful and Fast	*"… useful to researchers who do not have access to real data and want to generate synthetic data; ..one can see meaningful results in minutes…"* *"…useful but takes time to train…"* *"…useful for shown examples; requires generalization across several domains"* *"…useful but should add approximate completion time for given epochs.."*
Novelty	*"…makes AI accessible to layman people…"* *"…I find this project extremely interesting, especially the part where a user can manually tweak the graph to get necessary data points…"* *"…novel in the way it is combining various technologies and algorithms…"* *"…seems novel relative to physiological sensor data…"*
Usage Scenarios	*"…Machine learning thrives on large data sets, but labeled data are hard to get. Using this system, practitioners can test their model effectively. This system might be a great help for learning purposes…"* *"…A researcher who wants to generate synthetic data but does not know coding or does not have a good command on machine learning can use this easily…"* *"…Useful to do data exploration, data repairs, generating more data with similar characteristics"* *"..Use scenarios not made too clear by developers; however, it seems given we had a limited dataset of physiological readings, the tool can generate dataset for given task…"* *"…generating general purpose datasets.."*
Other Suggestions	*"…statistical graphs need to be bigger and logger option could be a pop up instead of distracting the user.."* *"…can include multiple GAN architectures…"* *"…more context is needed to evaluated the usefulness of the tool. Improve the readability and intuition behind the graphs…"* *"…utility tool should be added to check performance of deep learning models on synthetic data on the fly…"* *"…maybe avoid folder compression requirement before feeding to GAN…"*

Lessons Learnt

- Users appreciate the meaningfulness and impact of the tool, especially the controllable and collaborative aspects.
- Users want to check the validity of synthetic datasets on the fly with tertiary models apart from specifying corrections.
- Users want to explore several GAN models before taking a decision.
- The UI requires additional explainability tools and fine-tuning:
  - why signals were generated the way they look
  - the context of the statistical parameters and distributions
  - use more advanced UI elements to reduce clutter.

THANK YOU

https://github.com/swapnilsayansaha/ECE209AS_Fall2020/tree/main/Bake_off_2-GUI_GAN

Contributions:

- Viacheslav Inderiakin: Application frontend design and integration of all the parts.
- Swapnil Sayan Saha: Tensorflow backend design and general project directions.

Discussion

- Novelty, diversity and utility (w.r.t. user input parameters and corrections) are three numerical controllability and collaboration parameters that we have proposed to ensure "*a user can freely control the generative process and obtains results that match their expectation*". Do you have any other metrics in mind that can do the same?

- The framework currently deals with data processing but not data collection. Can you visualize a framework that will guide non-experts in any domain starting from data collection until model deployment?

- How can this framework be expanded for images? (keep in mind the framework must generalize for any application like the one proposed)