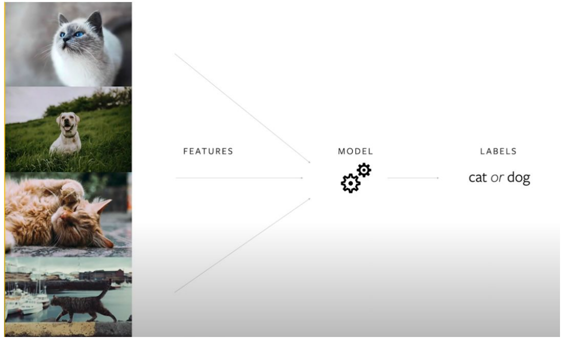
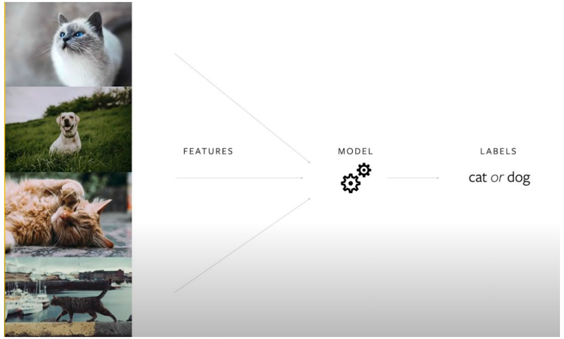
# Tutorial on Secure Multi Party Computation

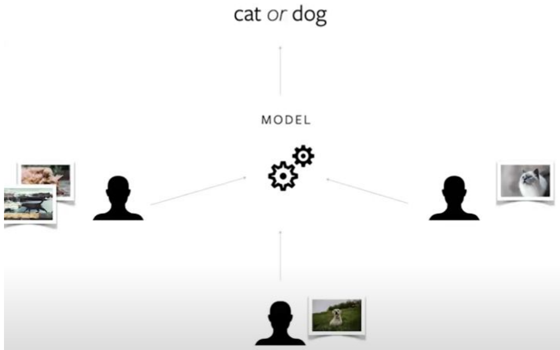
Privacy Enhancing Technologies (PETs)

# Machine Learning

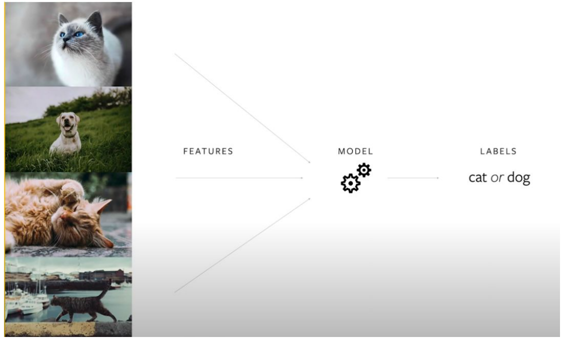


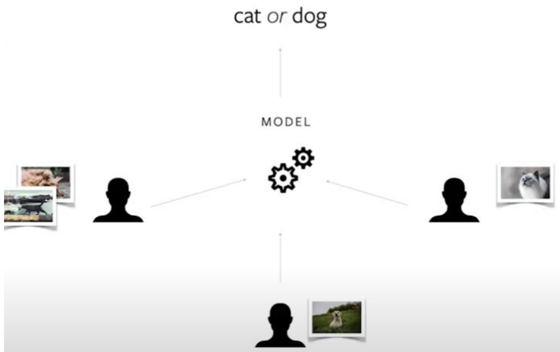
# Machine Learning

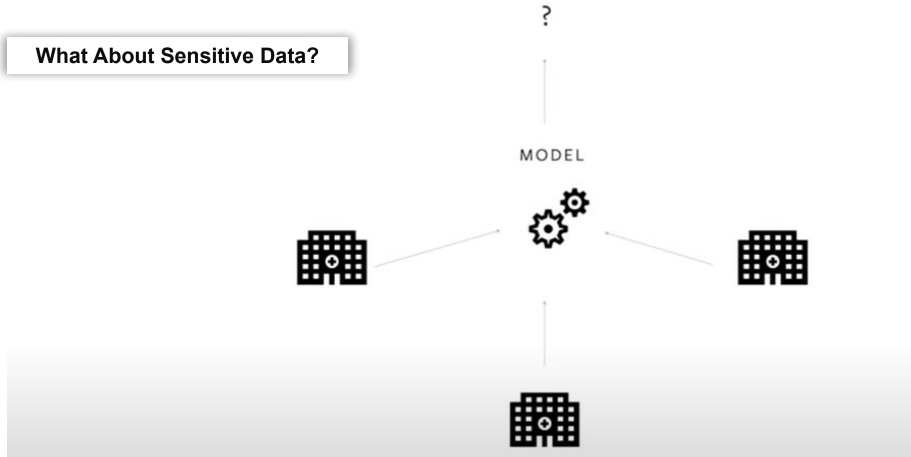




# Machine Learning

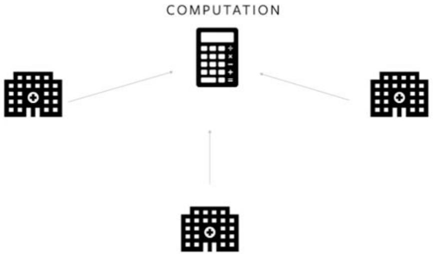





**What About Sensitive Data?**

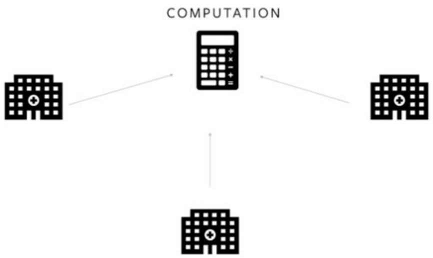
# Machine Learning with MPC

Secure Multi Party Computation

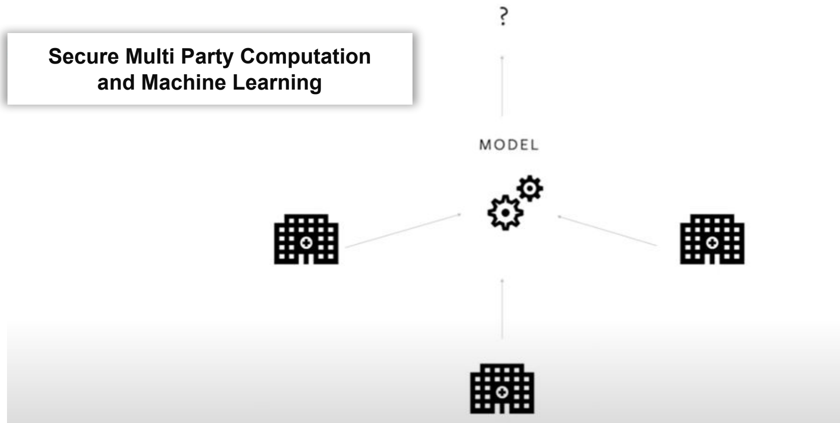


# Machine Learning with MPC

**Secure Multi Party Computation**



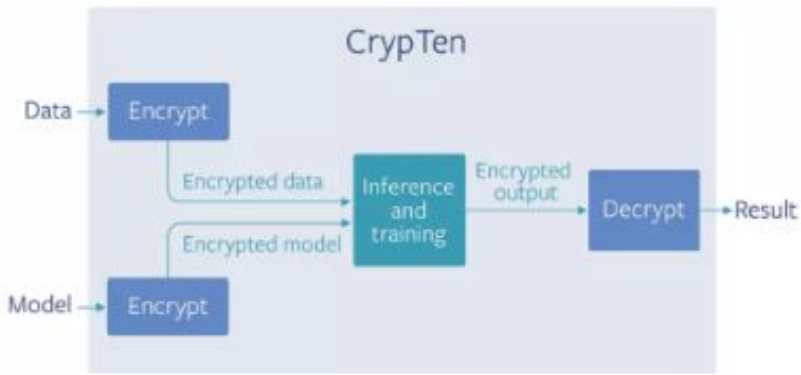
**Secure Multi Party Computation and Machine Learning**



# CrypTen

https://crypten.ai/

- CrypTen is a machine learning framework built on PyTorch that enables you to easily study and develop machine learning models using secure MPC.
- CrypTen allows you to develop models with the PyTorch API while performing computations on encrypted data.
- Different parties can contribute information to the model or measurement without revealing what they contributed.



## Secure Computations

- **Addition: (Code File: arithmetic.py)**
  - $z = x + y$ is computed as $[z] = [x] + [y]$ by each party

- **Multiplication: (Code File: beaver.py)**
  - Implemented using random Beaver triple ([a], [b], [c])
  - $[e] = [x] - [a]$ ; $[d] = [y] - [b]$
  - $[xy]_1 = [c] + e[b] + [a]d + ed$ ; $[xy]_2 = [c] + e[b] + [a]d$

- **Comparators: (Code File: logic.py)**
  - Evaluating $[z < 0]$:
    - Convert $[z]$ to binary secret-share ⟶ $[\![z]\!]$
    - Extract the sign bit: $[\![b]\!] = [\![z]\!] >> (L - 1)$
    - Convert bit $[\![b]\!]$ to an arithmetic share $[b]$
  - Compare Two Values:
    - $[x < y] = ([x] - [y]) < 0$

# Secure Computations

- **Comparators:**
  - Sign Function: **(Code File: logic.py)**
    - $\mathrm{sign}([x]) = 2 \cdot [x > 0] - 1$
  - Absolute Value: **(Code File: logic.py)**
    - $|[x]| = [x] \cdot \mathrm{sign}([x])$
  - ReLU Activation: **(Code File: logic.py)**
    - $\mathrm{ReLU}([x]) = [x] \cdot [x > 0]$
  - Multiplexer / Conditional Selection:
    - $[c\ ?\ x : y] = [c] \cdot [x] + (1 - [c]) \cdot [y]$

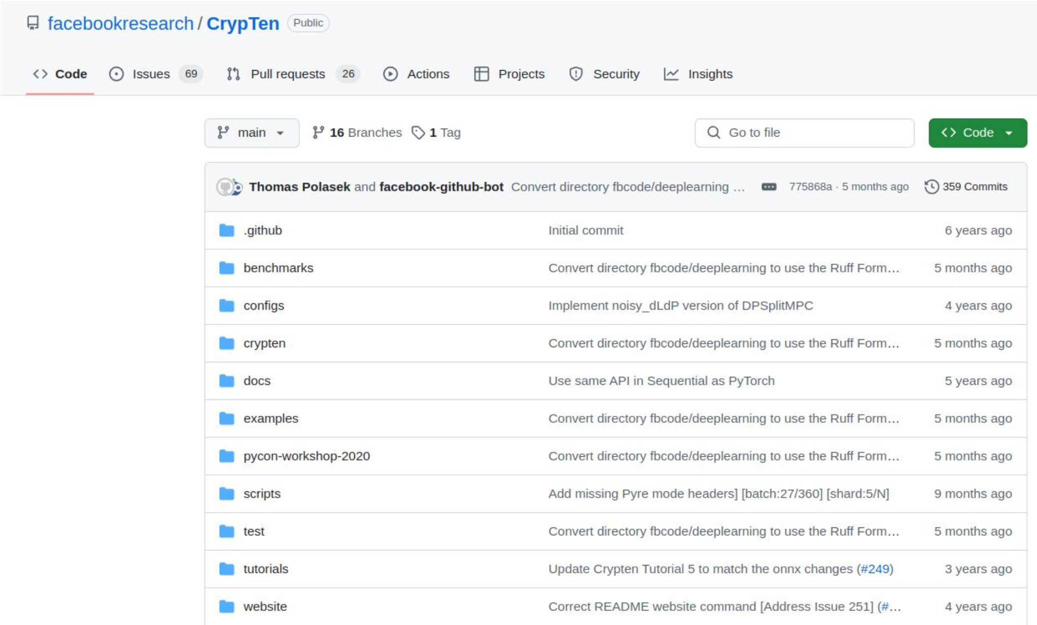
## Secure Computations

- **Conv1d/Conv2d ($\circledast$):** **(Code File: beaver.py)**
    - Computed as $c + e \circledast b + a \circledast d + e \circledast d$
    - Here e and d are masked inputs as: (This is same as beaver triples concept)
        - $e = x - a$
        - $d = y - b$
    - Same idea also works for:
        - matmul, conv_transpose1d, conv_transpose2d

- **MaxPool2D:** **(Code Files: pooling.py -> maximum.py)**
    - Input is reshaped to create a tensor of flattened sliding windows.
    - Each window is a vector over which the max is computed using secure comparison protocols.
    - Secure max is computed via repeated x > y comparisons over secret shares.
    - Padding is handled by inserting extremely negative values (-2^24) to ensure they are not selected.
    - Output is reshaped back to match the spatial dimensions

# CrypTen Library

https://github.com/facebookresearch/CrypTen/tree/main

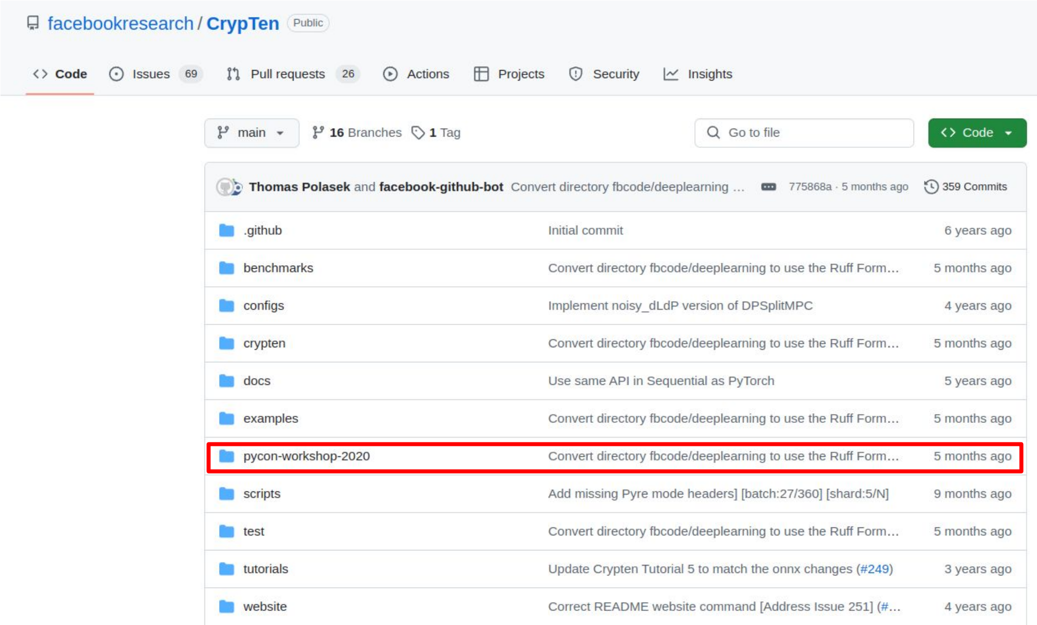


Thomas Polasek and facebook-github-bot Convert directory fbcode/deeplearning … 775868a · 5 months ago 359 Commits

| | | |
|---|---|---|
| .github | Initial commit | 6 years ago |
| benchmarks | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| configs | Implement noisy_dLdP version of DPSplitMPC | 4 years ago |
| crypten | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| docs | Use same API in Sequential as PyTorch | 5 years ago |
| examples | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| pycon-workshop-2020 | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| scripts | Add missing Pyre mode headers] [batch:27/360] [shard:5/N] | 9 months ago |
| test | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| tutorials | Update Crypten Tutorial 5 to match the onnx changes (#249) | 3 years ago |
| website | Correct README website command [Address Issue 251] (#… | 4 years ago |

# CrypTen Library

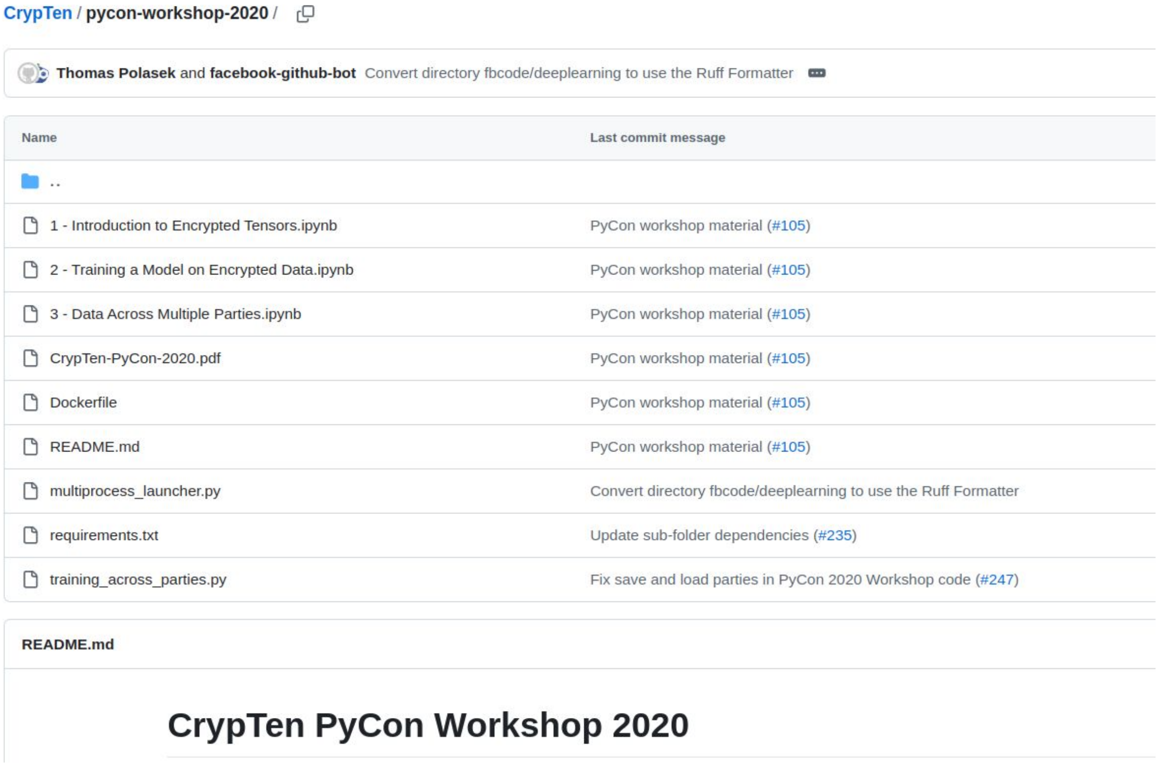
https://github.com/facebookresearch/CrypTen/tree/main



Thomas Polasek and facebook-github-bot Convert directory fbcode/deeplearning … 775868a · 5 months ago 359 Commits

| | | |
|---|---|---|
| .github | Initial commit | 6 years ago |
| benchmarks | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| configs | Implement noisy_dLdP version of DPSplitMPC | 4 years ago |
| crypten | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| docs | Use same API in Sequential as PyTorch | 5 years ago |
| examples | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| pycon-workshop-2020 | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| scripts | Add missing Pyre mode headers] [batch:27/360] [shard:5/N] | 9 months ago |
| test | Convert directory fbcode/deeplearning to use the Ruff Form… | 5 months ago |
| tutorials | Update Crypten Tutorial 5 to match the onnx changes (#249) | 3 years ago |
| website | Correct README website command [Address Issue 251] (#… | 4 years ago |

# CrypTen Library



CrypTen / pycon-workshop-2020 /

**Thomas Polasek** and **facebook-github-bot** Convert directory fbcode/deeplearning to use the Ruff Formatter

| Name | Last commit message |
|---|---|
| .. | |
| 1 - Introduction to Encrypted Tensors.ipynb | PyCon workshop material (#105) |
| 2 - Training a Model on Encrypted Data.ipynb | PyCon workshop material (#105) |
| 3 - Data Across Multiple Parties.ipynb | PyCon workshop material (#105) |
| CrypTen-PyCon-2020.pdf | PyCon workshop material (#105) |
| Dockerfile | PyCon workshop material (#105) |
| README.md | PyCon workshop material (#105) |
| multiprocess_launcher.py | Convert directory fbcode/deeplearning to use the Ruff Formatter |
| requirements.txt | Update sub-folder dependencies (#235) |
| training_across_parties.py | Fix save and load parties in PyCon 2020 Workshop code (#247) |

**README.md**

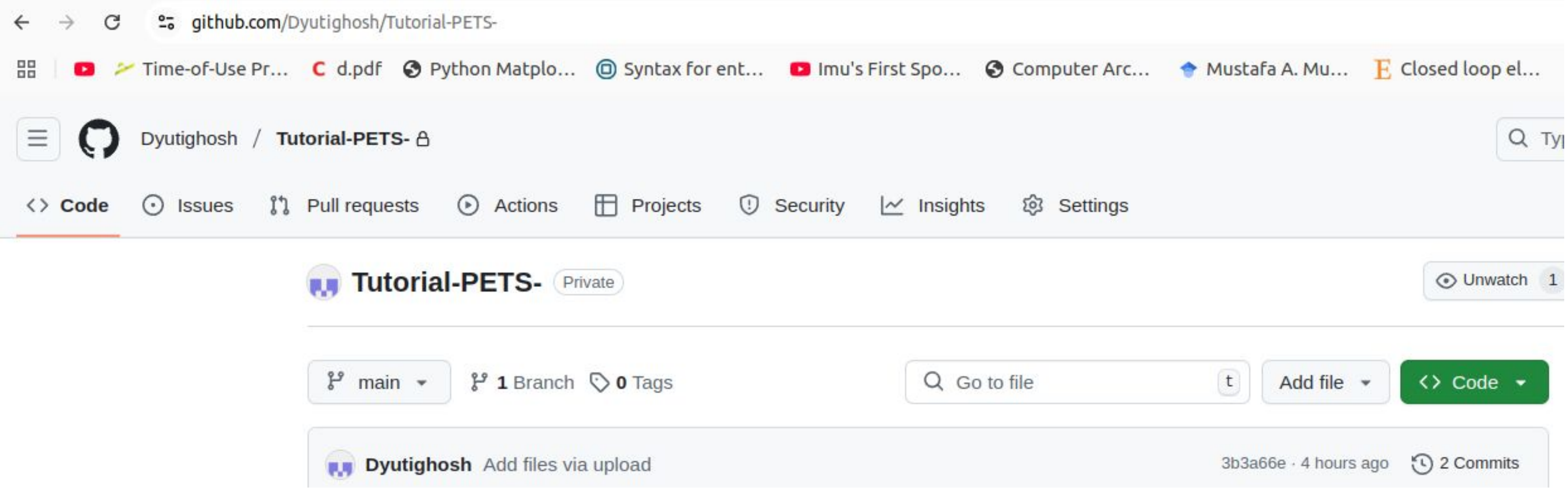
## CrypTen PyCon Workshop 2020

# Results (Timing and Accuracy using TinyCNN)

| Library | Time Taken for Inference | Accuracy of Inference |
|---|---|---|
| Concrete-ML<br>(Last Tutorial) | 154 seconds (Collab)<br>**25 seconds (local system)** | **100%** |
| Crypten<br>(2PC) | | |
| Crypten<br>(5PC) | **64.35 seconds** | **96.00%** |

# Results (Timing and Accuracy using TinyCNN)

| Library | Time Taken for Inference | Accuracy of Inference |
|---|---|---|
| Concrete-ML (Last Tutorial) | 154 seconds (Collab)<br>**25 seconds (local system)** | **100%** |
| Crypten (2PC) | **0.88 seconds** | **96.67%** |
| Crypten (5PC) | **64.35 seconds** | **96.00%** |



github.com/Dyutighosh/Tutorial-PETS-

Dyutighosh / Tutorial-PETS-

Tutorial-PETS- Private

Dyutighosh Add files via upload 3b3a66e · 4 hours ago 2 Commits

# Thank You

Contact Information: Soumyadyuti.ghosh@gmail.com