1. **PROJECT TITLE:**

**SConvA-Net: Siamese convolutional Autoencoder based attack detection with blockchain based multiparty big data sharing**

**2. HARDWARE REQUIREMENTS**

OS-Windows 10

RAM-8GB

ROM-More than 100 GB

GPU-Yes

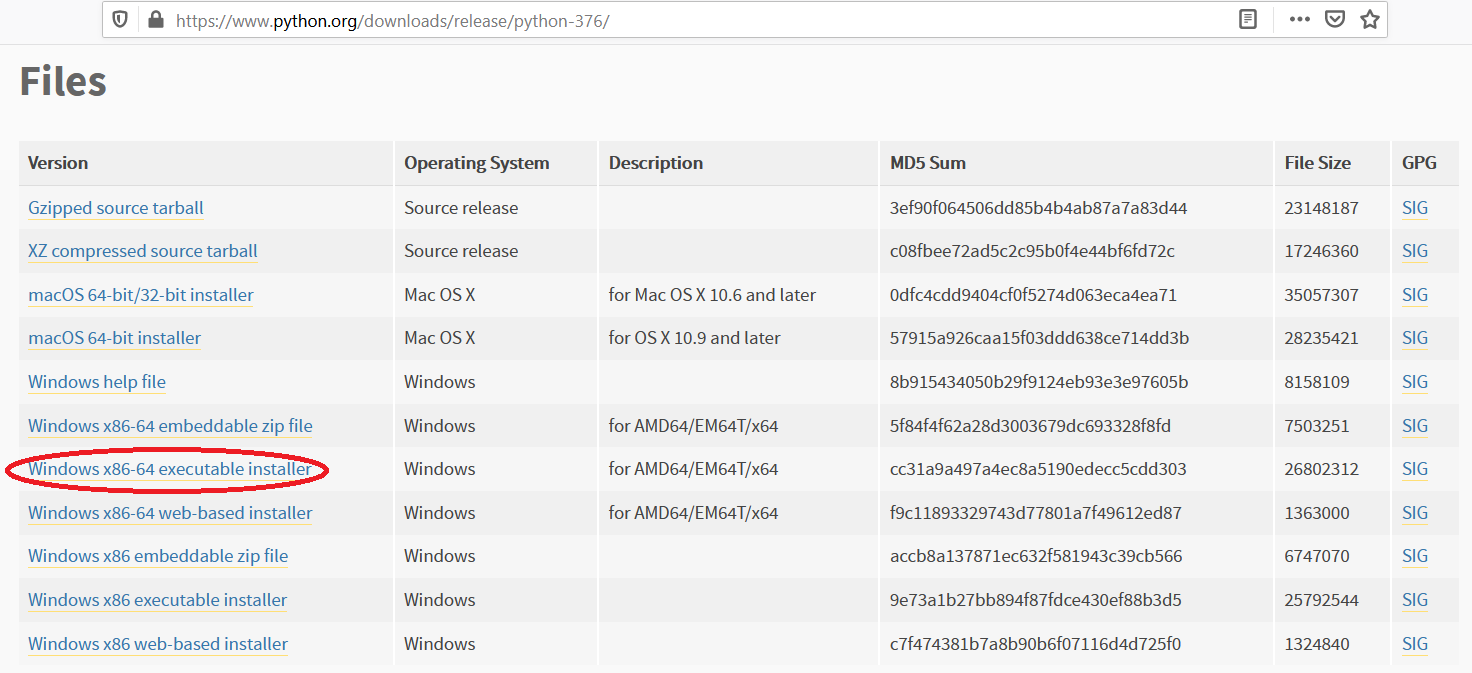
CPU-1.7 GHz

**3. SOFTWARE REQUIREMENTS**

Software name(**Python**): Version: 3.9.11

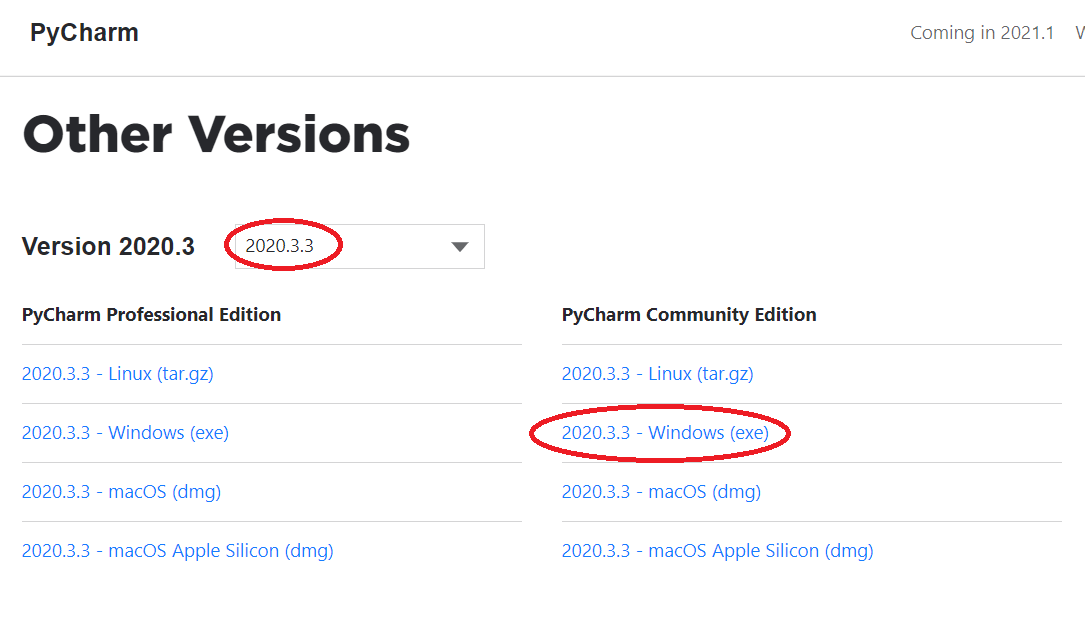
(Download link: <https://www.python.org/downloads/release/python-376/> )

Click -> Windows x86-64 executable installer.



Software name: **PyCharm**: Version: 2020.3.3

(Download link: <https://www.jetbrains.com/pycharm/download/other.html>)



(For installation procedure, please refer the doc “steps to install python.doc”)

**4. HOW TO RUN**

**Step 1**: Loading the project in PYCHARM

* Open pycharm
* Go to File, select Open browse the project from your drive and select it. So that the project will get loaded into the Pycharm.
* For the first time, Pycharm will take some time to load the settings.
* Please wait if any process is loading on the bottom of the screen.
* Check the Project Interpreter (File -> Settings -> Project: 218604-> Project Interpreter).

If this location “(C:\Users\---\AppData\Local\Programs\Python\Python39-64\python.exe) is not presented, then add this ‘python.exe’ from the installed location.

* In Pycharm Terminal(bottom left), type the comment “pip install -r requirements.txt”

**Step 2**: Run the program and getting the results

* From 'current project folder' window in pycharm, Open 218604**-> Main->GUI.py**’ and click run button
* In GUI window,
* 1) Select Training data(%)(eg:60,70,80,90) or K Fold(eg:5,6,7,8)

4) Click START, after some time the result will be displayed

5) Click Run Graph to view the current result graph.

[Expected Execution time expected: **15 – 20 minutes**]

* **Step 3**: Generate the graphs plotted in the paper
* From 'current project folder' window in pycharm, open ‘218604-> Main->Result\_graphs.py’, and click run button.

**5. IMPORTANT PYTHON FILE AND DESCRIPTION:**

**Main-> GUI.py**: User Interface, code starts here

**Main-> Run.py**: Main code

**Main->From\_Previous\_work ->Map\_Reducer.py :** Under Map reduce framework, in mapper phase, the will be based on identity and attribute based honey encryption algorithm (IABHE), which will be a modified encryption algorithm of the work given in [“Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective”] by including the identity and the new key generation procedure, where the key will be generated by deep learning. Here, we used DSNN for the key generation process – and in the reducer phase, the encrypted data from the mapper will be further increased its robustness by doing the polynomial interpolation.(from paper 2)

After data sharing, to maintain security implement attack detection

**Main->Data\_Normalization.py :** data normalization using Z-score

**Main->Feature\_Selection.py :** feature selection using Relief technique (“Relief F-Based Feature Ranking and Feature Selection for Monitoring Induction Motors”)

**Proposed\_SConvA\_Net ->SCNN.py , DSA.py** attack detection using Siamese convolutional Autoencoder network (SConvA-Net), combination of SCNN and DSA

**Main-> Result\_graphs.py**: displays graphs in paper.