MANTHAN 2021

Premier Hackathon for National Security

MANTHAN
राष्ट्रीय सुरक्षा सर्वोपरि

Azadi Ka Amrit Mahotsav

DEEPFAKE CONTENT DETECTION USING ADVANCED GAN

RATHINAM COLLEGE OF ARTS AND SCIENCE

TEAM NAME : THE_FANTASTIC_5
PSID : INTL-FCD-15
TEAM MENTOR NAME : NAREN J
TEAM LEADER NAME : JASMINE AK

TEAM MEMBERS:
1. AKASH R
2. GAYATHRI M
3. MAHALAKSHMI G
4. SARAVANAVEL V

RATHINAM GROUP OF INSTITUTIONS

PROBLEM STATEMENT : INTL-FCD-15

MANTHAN राष्ट्रीय सुरक्षा सर्वोपरि

Azadi Ka Amrit Mahotsav

IDENTIFICATION OF ARTIFICIALLY GENERATED DEEP FAKE CONTENT

Deepfake is a technique that uses deep learning algorithm to create fake images usually by swapping a person's face from a source image into another person's face in a target image, the algorithm can create fake images that humans cannot distinguish them from authentic ones.

MOTIVATION

- Deep fake technology has opened doors to many new possibilities of picture generation but also raised many issues of moral and legal matters

- The Motive is to get aware of fake images through Deep Learning technology.

IDENTIFICATION OF ARTIFICIALLY GENERATED DEEP FAKE IMAGE CONTENTS

1. Deep fake technology has opened doors to many new possibilities of picture generation but also raised many issues of moral and legal matters

2. The Motive is to get aware of fake images through Deep Learning technology

3. To build a Deep Learning Model which classifies real and fake images.

DEEP FAKE CONTENT DETECTION

- BASELINE

DEEP LEARNING (DL) :

Deepfakes uses deep learning technology to manipulate images, videos, audios of a person that humans cannot differentiate them from the real one.

In deepfake AI, deep learning algorithms that teach themselves how to solve problems with large data sets, are used to swap faces in videos, images, and other digital content to make the fake appear real.

SOLUTION STACK (Continuation)

GENERATIVE ADVERSARIAL NETWORKS(GAN) :

GAN is an algorithmic architectures that use two neural networks, pitting one against the other (thus the “adversarial”) in order to generate new synthetic instances of data.

CONVOLUTIONAL NEURAL NETWORKS(CNN) :

Convolutional Neural Network(CNN) is a Deep Learning algorithm which can take in an input image, assign importance to various aspects in the image and be able to differentiate one from the other.

DEEPFAKE IMAGE CONTENTS

OBJECTIVES :

IMAGE DETECTION :

- Idea Introduction
- Outcome And Approach
- Architecture
- Vision

VIDEO DETECTION :

- Idea Introduction
- Outcome And Approach
- Architecture
- Vision

CNN ARCHITECTURE (DISCRIMINATOR)

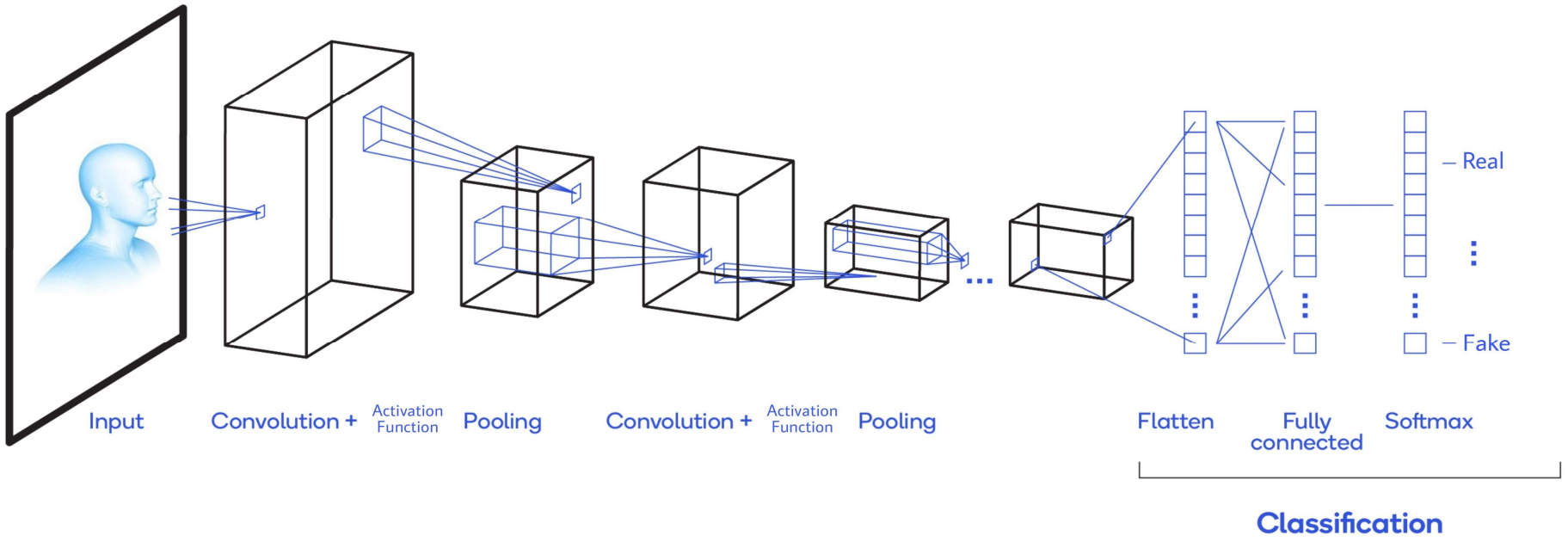
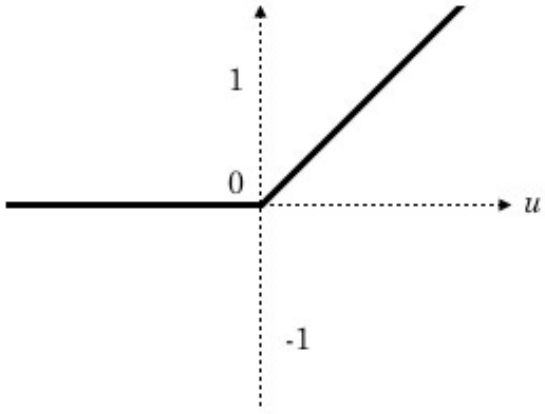


Figure 1: CNN Architecture

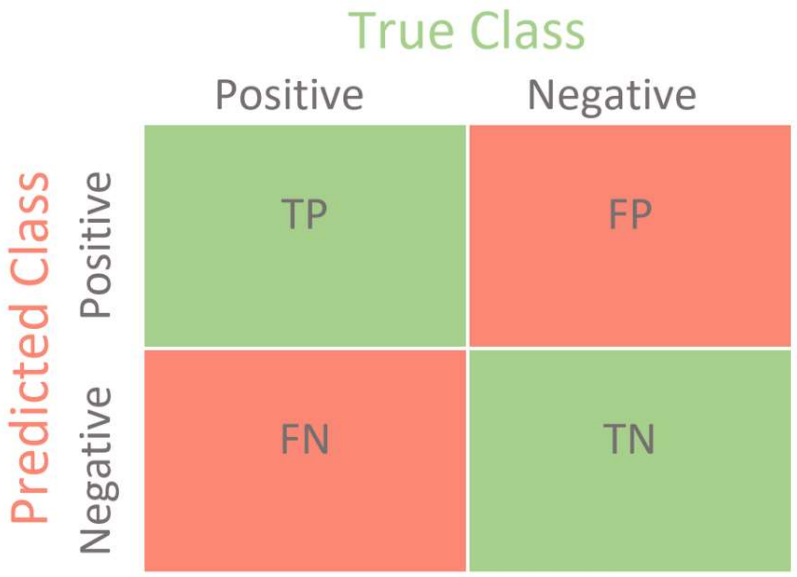
Source : Own Image

ACTIVATION FUNCTION USED FOR CONVOLUTION LAYERS

RELU Activation Function



EVALUATION MATRIX



PRECISION = TP / (TP + FP)

RECALL = TP / (TP + FN)

DATASET

- 140 K Real and Fake Faces →From Kaggle
- 70 K Real from Flickr
- 70 K Fake from GAN generated

Train Set	Validation Set	Test Set
50 K Images	10 K Images	10 K Images

SAMPLE DATASET

VISION

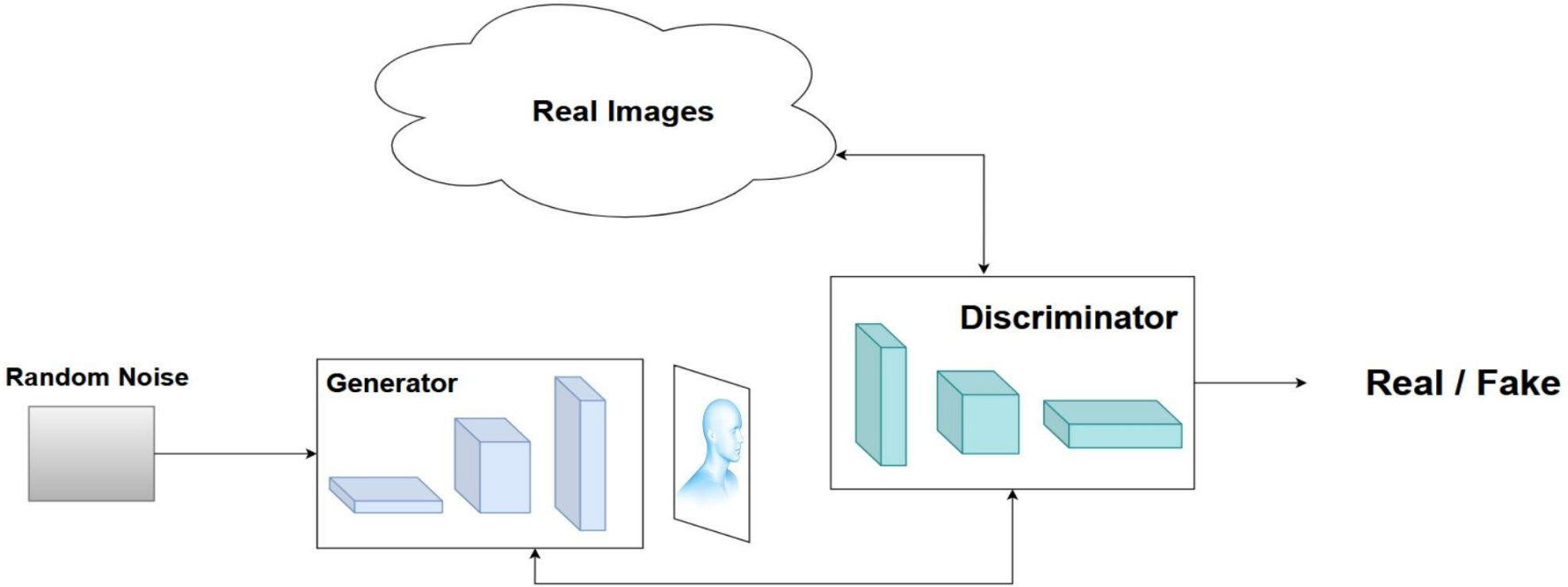
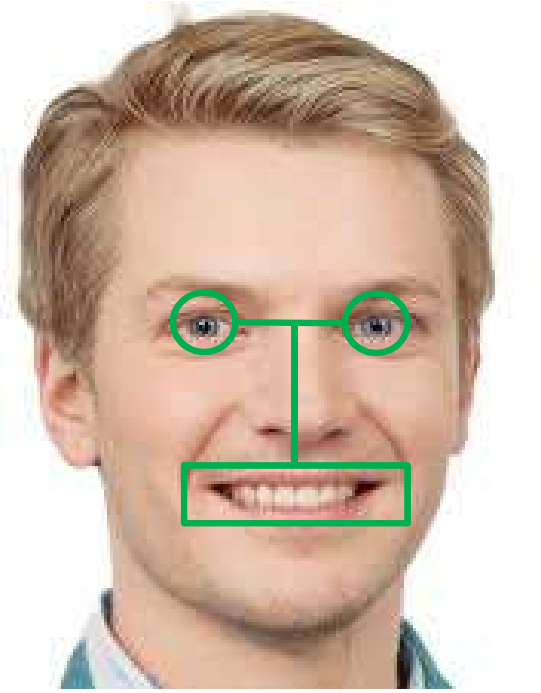


Figure 2 : Overview Of Model

Source : Own Image

APPROACH



- POSITION OF EYE
- POSITION OF NOSE
- POSITION OF LIPS

ACHIEVED ACCURACY

MODEL ON REAL AND ARTIFICIALLY GENERATED DEEPFAKE IMAGE DETECTION

86%→ 91%→ 96%

IDEA INTRODUCTION

- Deepfakes are synthetic media in which a person in an existing video is replaced with someone else's likeness
- It can create videos of public figures doing or saying things they never did
- The creator behind those videos has turned it into a profession by launching a company called Metaphysic to make hyper realistic videos with AI.

OUTCOME

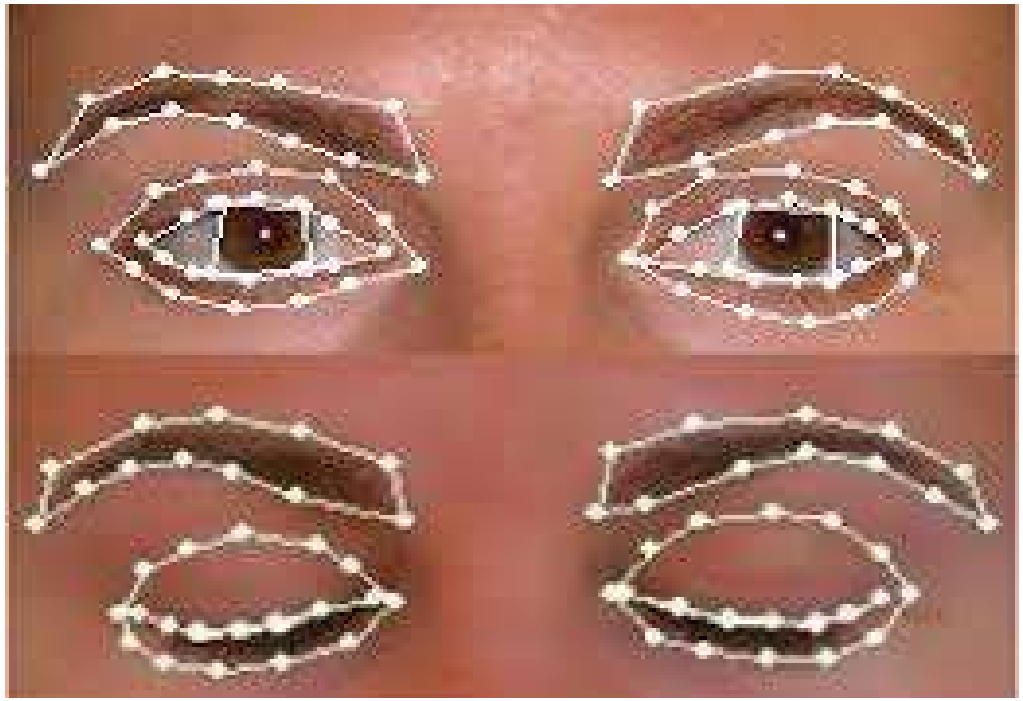
Our outcome is to categorize between real and fake or artificially generated videos which more likely as real ones using Generative Adversarial Network.

Deepfake digital videos have serious negative impacts on news integrity, legal forensics and social security.

In order to detect deep fake digital videos more accurately, a hybrid Generative Adversarial Networks (GAN) is proposed.

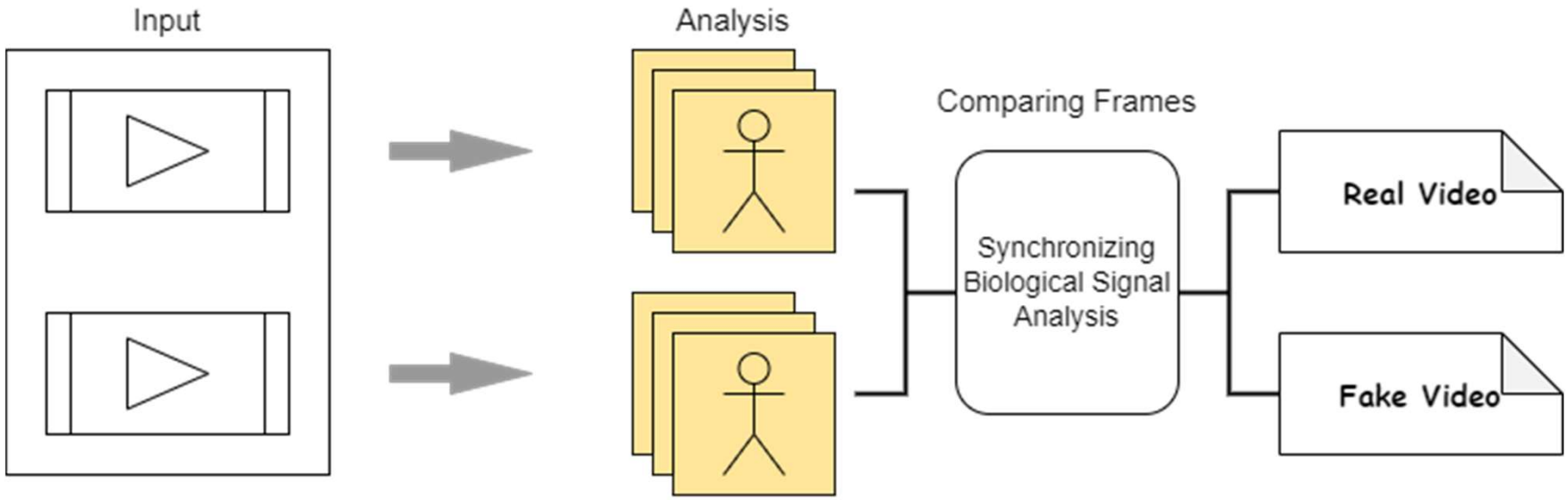
APPROACH

- Videos are converted into frames
- Each frame is considered as image



Eye Movement and Blink-ness comparison in real and fake videos

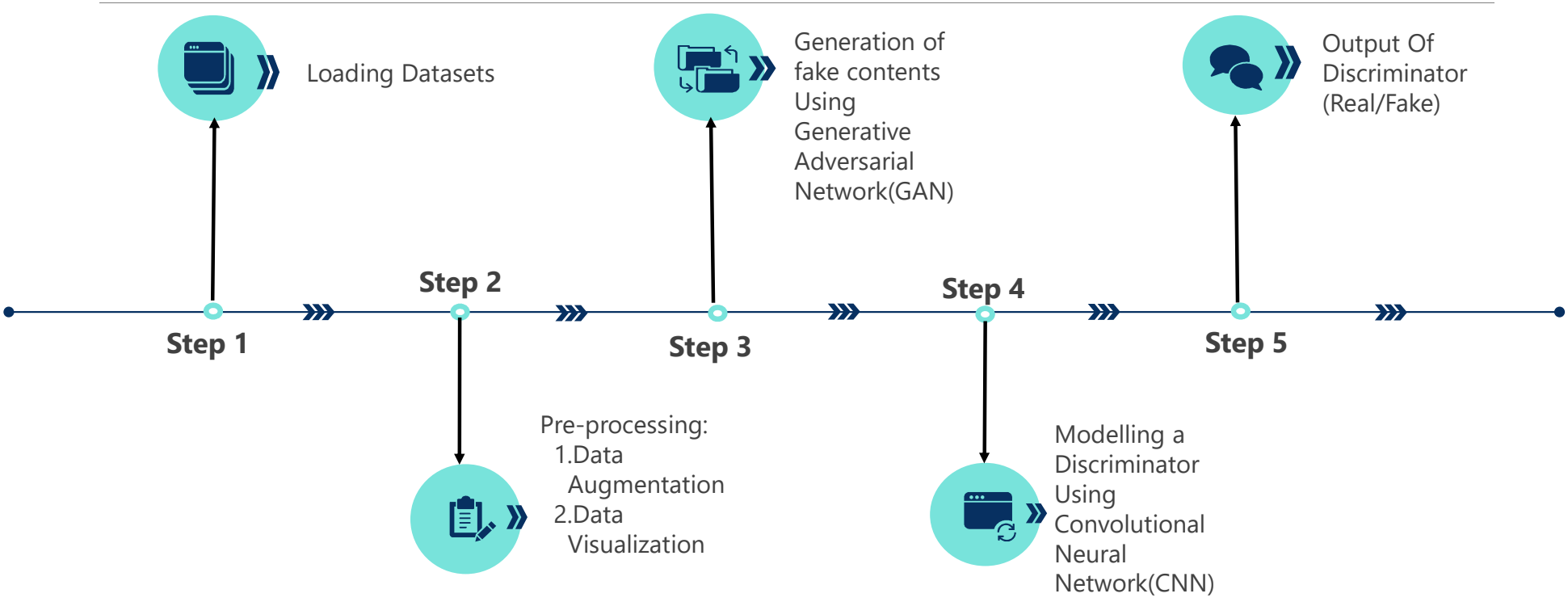
ARCHITECTURE (GENERATOR)



Source : Own Image

RATHINAM GROUP OF INSTITUTIONS

DEVELOPMENT PIPELINE

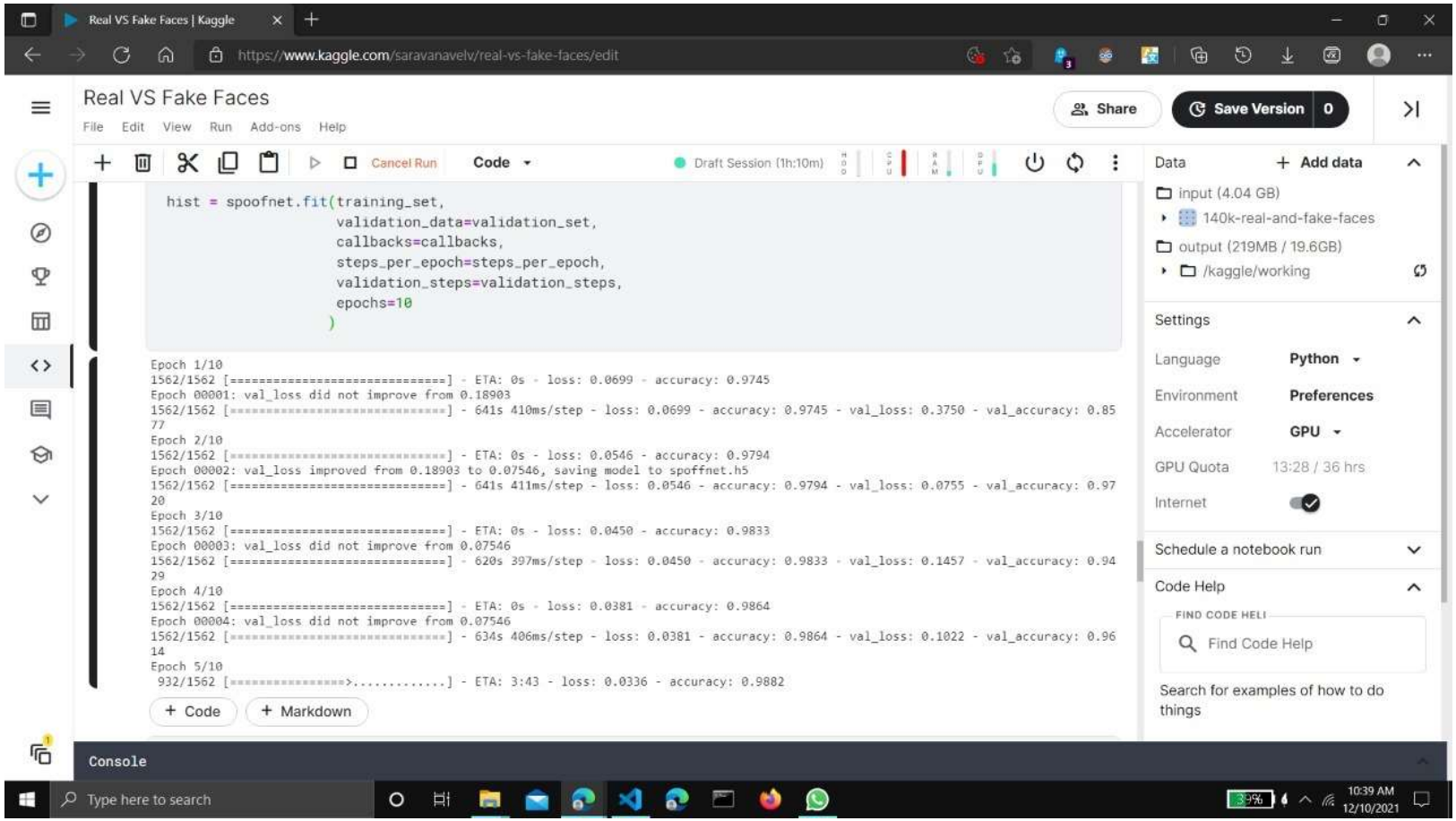


RATHINAM GROUP OF INSTITUTIONS

TRAINING AND RESULTS

MANTHAN राष्ट्रीय सुरक्षा सर्वोपरि

Azadi Ka Amrit Mahotsav

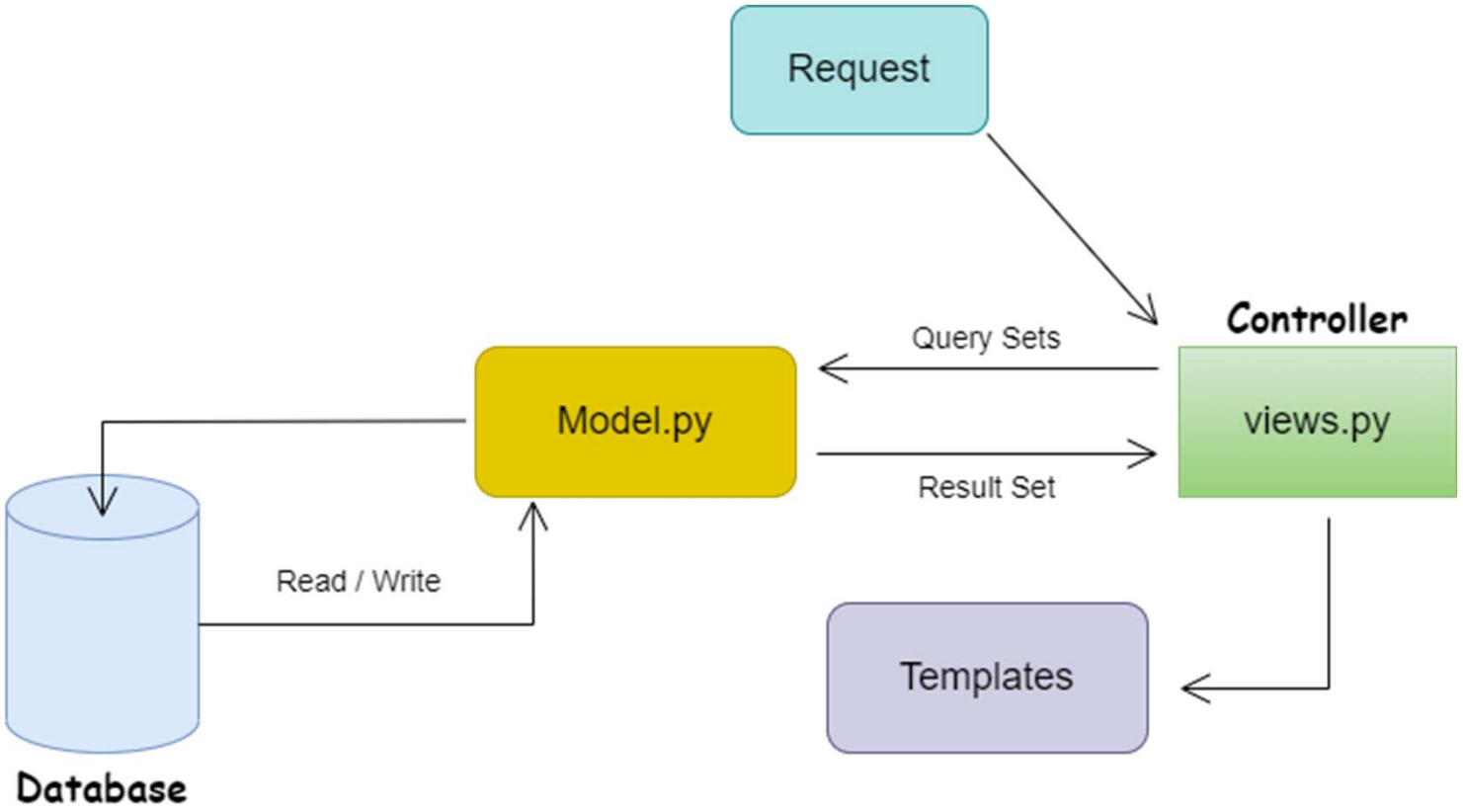


DEPLOYMENT OF OUR MODEL

django + Model

(as web app)

WORKING OF DJANGO



Source : Own Image

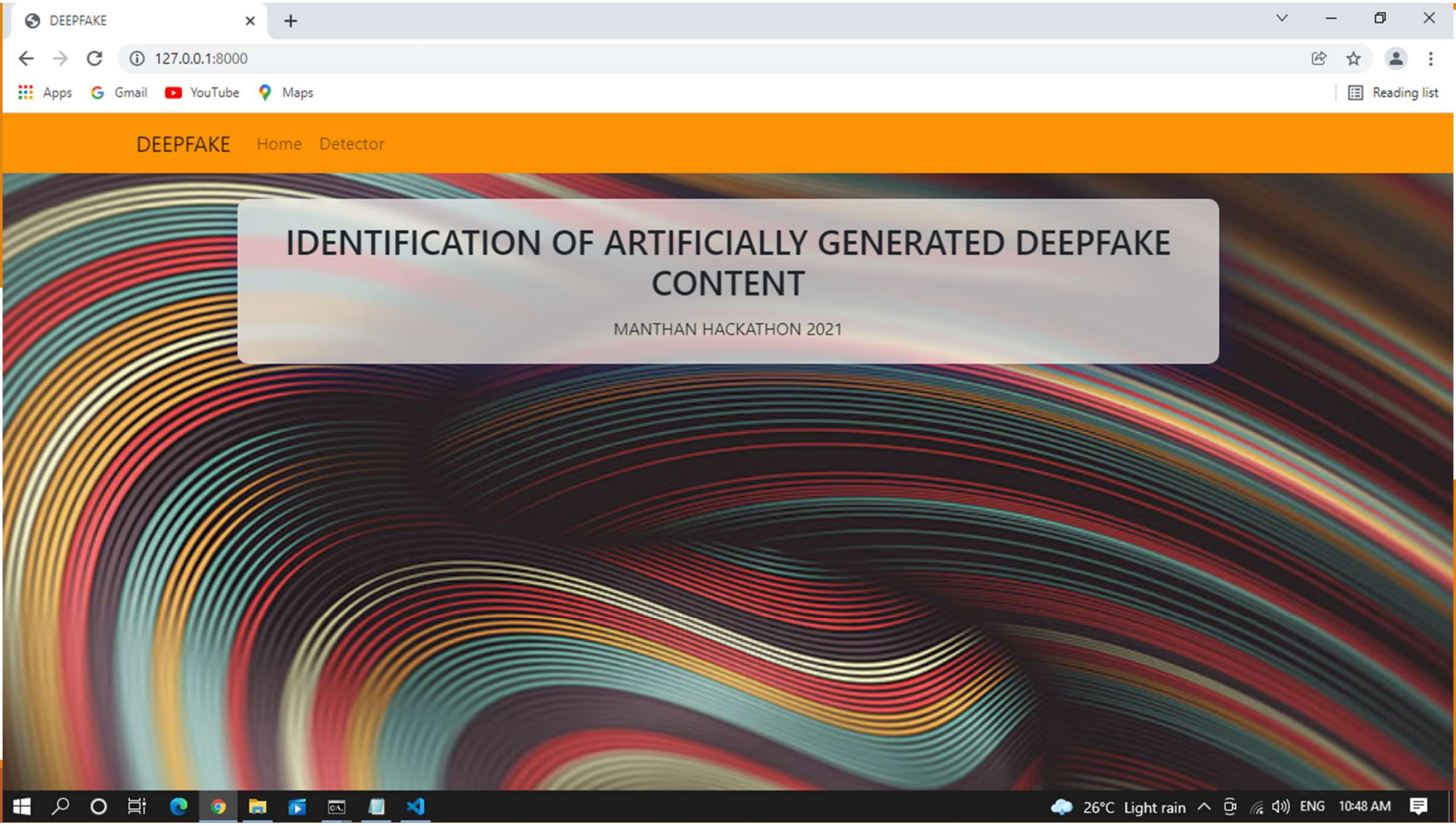
Django currently supports two interfaces:

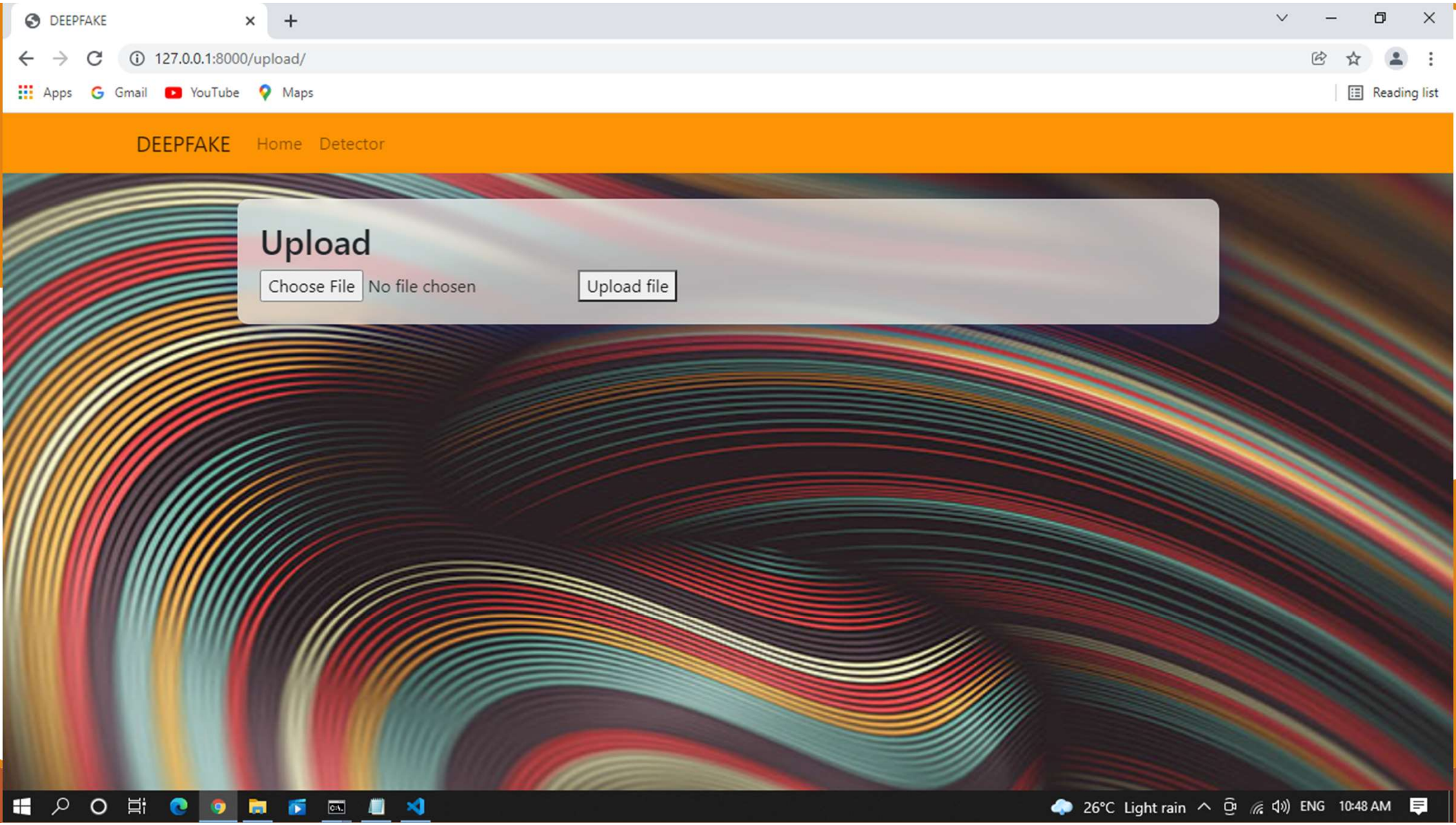
- WSGI - Web Server Gateway Interface
- ASGI - Asynchronous Server Gateway Interface

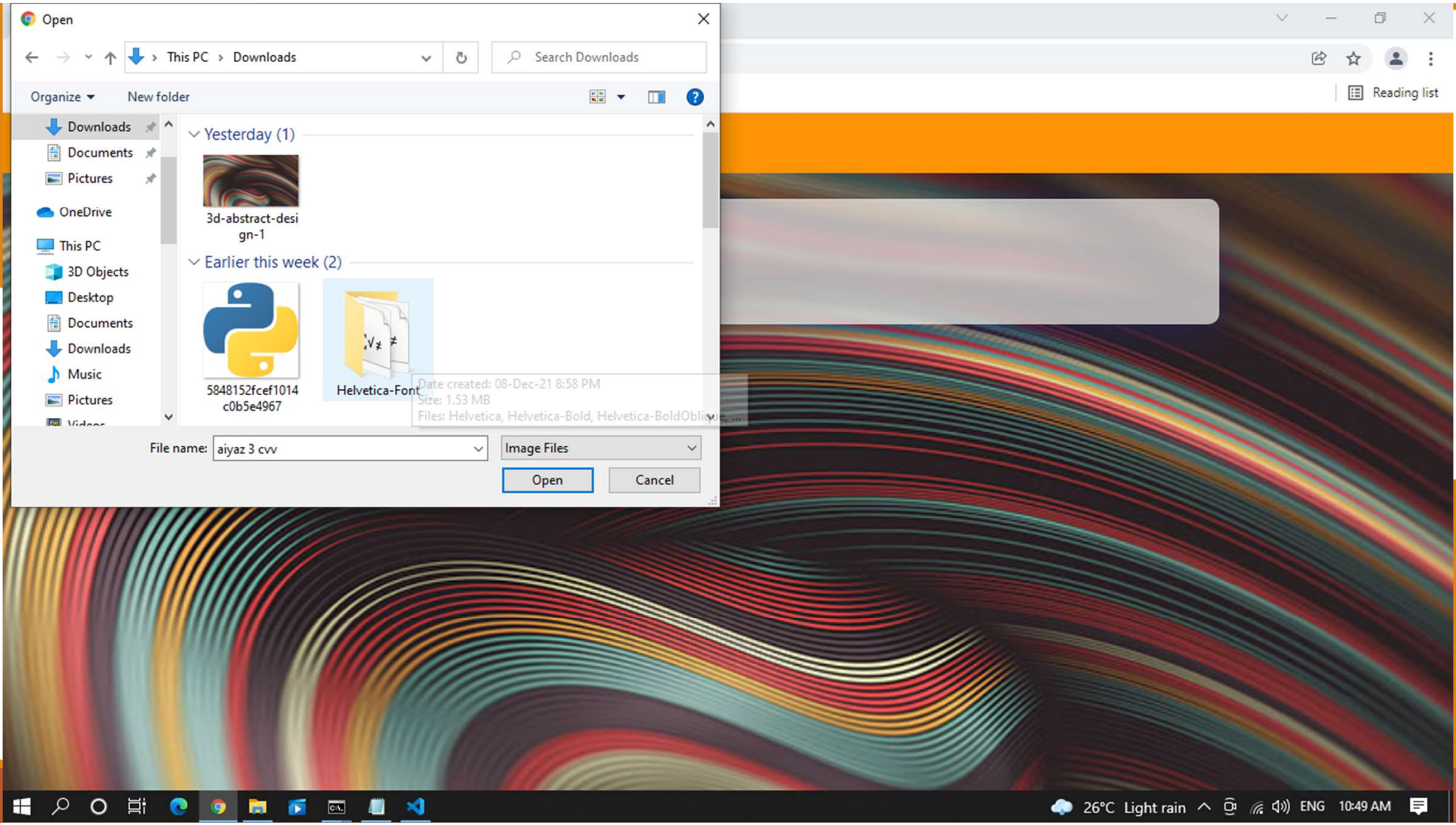
Communication between the web server and the web applications in most of the python web frameworks

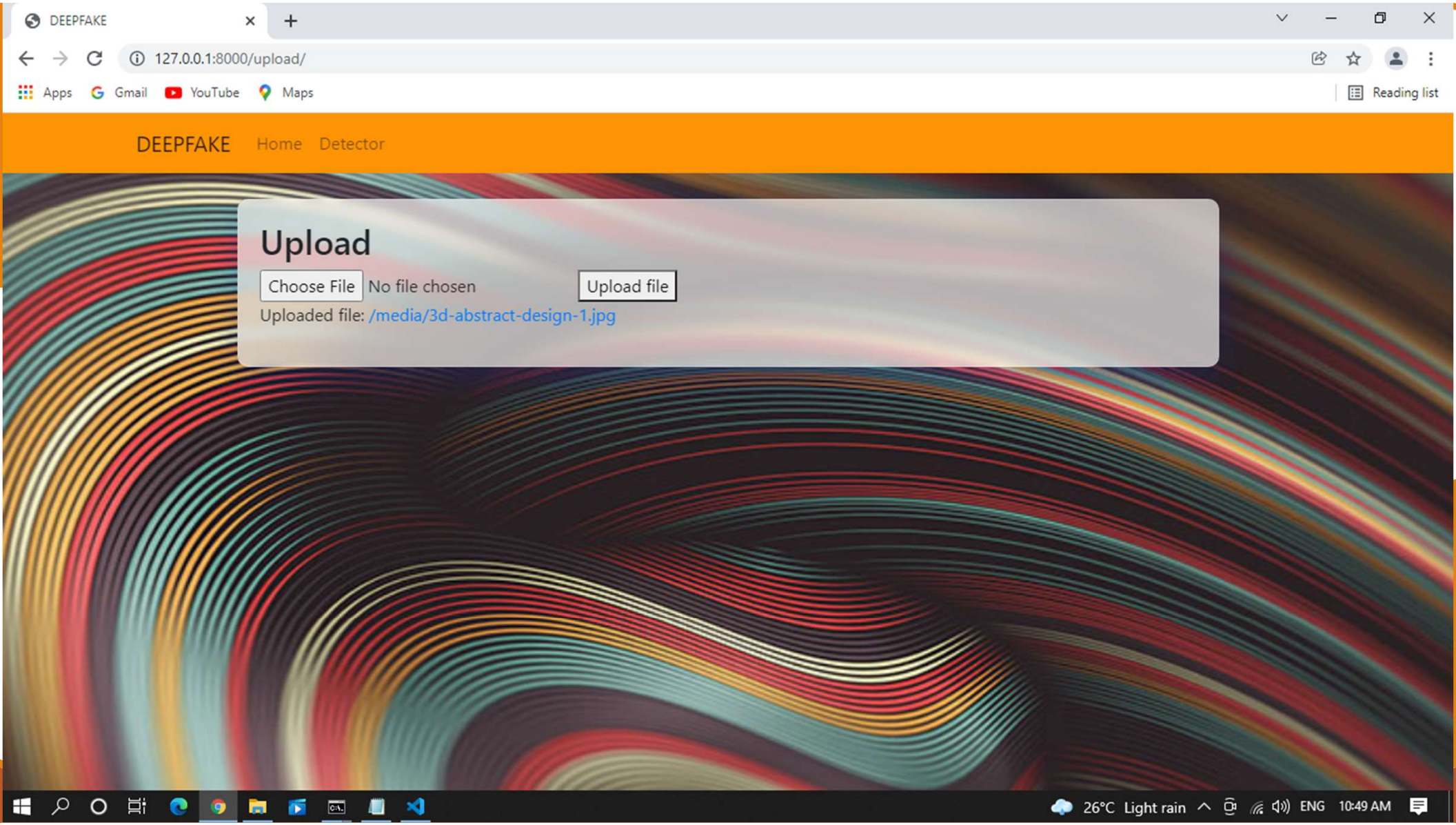
SECURITY FEATURES IN DJANGO

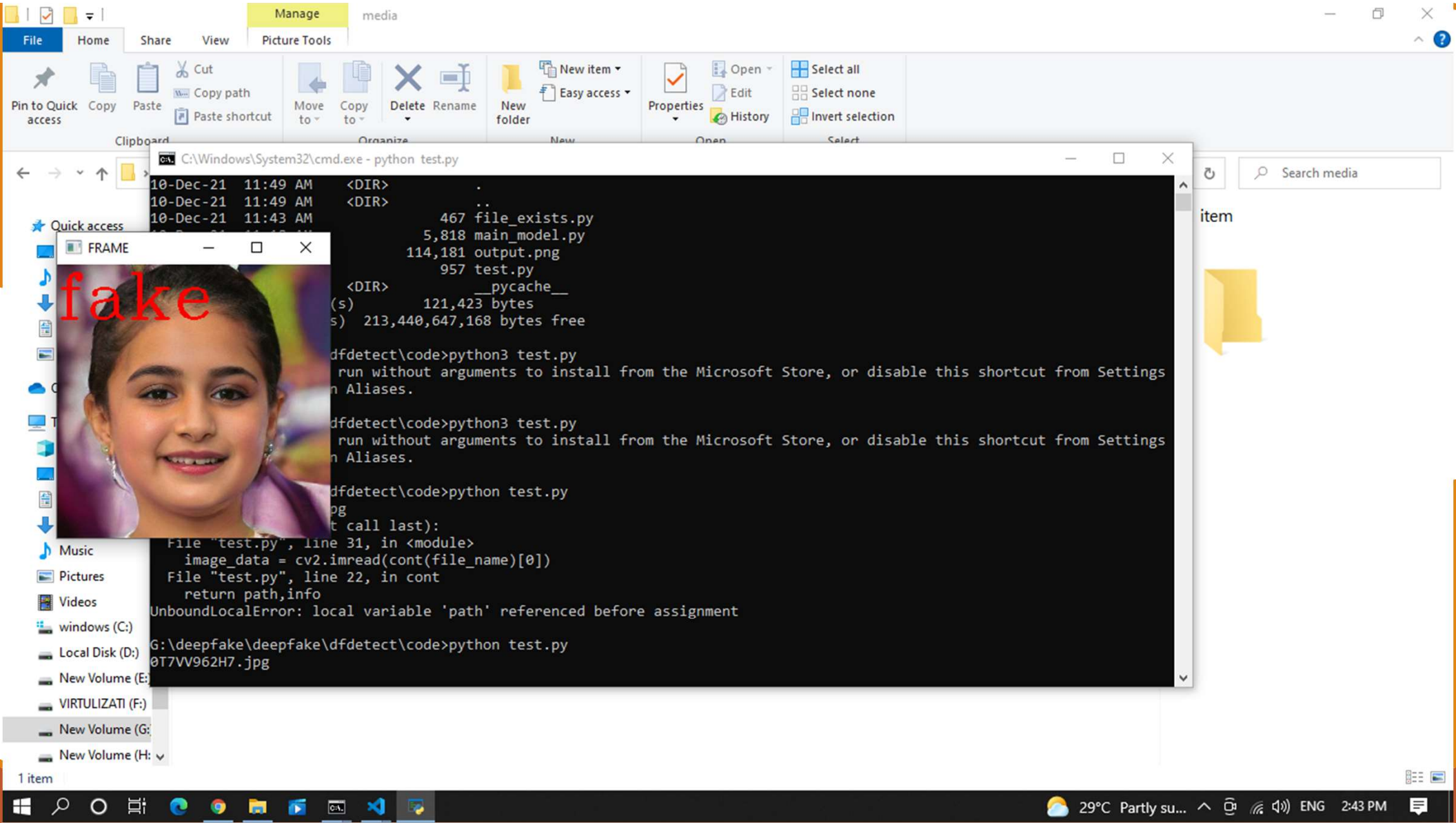
- Cross site scripting (XXS) protection
- Cross site request forgery (CSRF) protection
- SQL injection projection
- Clickjacking protection
- SSL / HTTPS


DEEPFAKE
127.0.0.1:8000
Apps
Gmail
YouTube
Maps
Reading list
DEEPFAKE
Home
Detector
IDENTIFICATION OF ARTIFICIALLY GENERATED DEEPFAKE CONTENT
MANTHAN HACKATHON 2021
26°C
Light rain
ENG
10:48 AM


DEEPFAKE
127.0.0.1:8000/upload/
Apps
Gmail
YouTube
Maps
Reading list
DEEPFAKE
Home
Detector
Upload
Choose File
No file chosen
Upload file
26°C
Light rain
ENG
10:48 AM


Open
This PC › Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Yesterday (1)
3d-abstract-design-1
Earlier this week (2)
5848152fcef1014c0b5e4967
Helvetica-Font
Date created: 08-Dec-21 8:58 PM
Size: 1.53 MB
Files: Helvetica, Helvetica-Bold, Helvetica-BoldOblique, ...
File name:
aiyaz 3 cvv
Image Files
Open
Cancel
Reading list
26°C Light rain
ENG
10:49 AM


DEEPFAKE
127.0.0.1:8000/upload/
Apps
Gmail
YouTube
Maps
Reading list
DEEPFAKE
Home
Detector
Upload
Choose File
No file chosen
Upload file
Uploaded file: /media/3d-abstract-design-1.jpg
26°C
Light rain
ENG
10:49 AM


Manage
media
File
Home
Share
View
Picture Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Search media
item
Quick access
Music
Pictures
Videos
windows (C:)
Local Disk (D:)
New Volume (E:)
VIRTULIZATI (F:)
New Volume (G:)
New Volume (H:)
1 item
C:\Windows\System32\cmd.exe - python test.py
10-Dec-21 11:49 AM <DIR> .
10-Dec-21 11:49 AM <DIR> ..
10-Dec-21 11:43 AM 467 file_exists.py
5,818 main_model.py
114,181 output.png
957 test.py
<DIR> __pycache__
(s) 121,423 bytes
s) 213,440,647,168 bytes free
dfdetect\code>python3 test.py
run without arguments to install from the Microsoft Store, or disable this shortcut from Settings
n Aliases.
dfdetect\code>python3 test.py
run without arguments to install from the Microsoft Store, or disable this shortcut from Settings
n Aliases.
dfdetect\code>python test.py
pg
t call last):
File "test.py", line 31, in <module>
image_data = cv2.imread(cont(file_name)[0])
File "test.py", line 22, in cont
return path,info
UnboundLocalError: local variable 'path' referenced before assignment
G:\deepfake\deepfake\dfdetect\code>python test.py
0T7VV962H7.jpg
FRAME
fake
29°C Partly su...
ENG
2:43 PM

RATHINAM
GROUP OF INSTITUTIONS

MANTHAN
राष्ट्रीय सुरक्षा सर्वोपरि

Azadi ka Amrit Mahotsav

THANK YOU