# YOUTUBE TAB CLASSIFICATION AND USER PRIVACY USING FEDERATED LEARNING

Ankita Rajput 2020BITE030

Ishita Sharma 2020BITE013

02-07-2024

# INTRODUCTION

- Monitoring student engagement and productivity on YouTube is crucial for improving learning outcomes and providing personalized support.
- A privacy-preserving architecture is proposed to detect whether students are utilizing their time on their computer or wasting it while the user's privacy is protected with federated learning.
- A dataset containing screenshots of different YouTube activities of students is used to classify them into categories using several pre-trained models.
- By distributing the learning process across YouTube and ensuring that sensitive data remains local, our approach ensures the privacy of the end user.

# PROBLEM STATEMENT

- We aim to address this challenge by developing a privacy-preserving solution for YouTube activity tracking using federated learning techniques.
- This decentralized learning paradigm ensures that sensitive user data remains on the local device, thus mitigating privacy risks associated with centralized data collection.
- Ensuring student engagement and productivity in YouTube environment while preserving user privacy poses a significant challenge.
- Traditional monitoring methods often compromise privacy, raising ethical concerns and hindering widespread adoption.

# OBJECTIVES

- Privacy Preservation
- Classification
- Evaluation and Validation
- Real-time Monitoring
- Model Update and Improvement

# LITERATURE SURVEY

| Paper | Method | Dataset | Accuracy | Limitations |
|---|---|---|---|---|
| Using screen capture to study user research behavior | Video screen capture technology to analyze user behavior | N/A | N/A | Resource expensive, No automatic detection |
| Log files for Learning Analytics from mobile screen recordings | Computer vision based machine learning to track activity of students from mobile screen recordings | 118 videos | N/A | Continuous mobile screen recording not practical, Slows down performance, Raises privacy concerns |
| Tracking digital device utilization from screenshot analysis using deep learning | Deep learning based activity tracking from computer screenshots | 4000 Screen-shots | 95.4% | Do not consider user privacy |

# PRIVACY PRESERVATION

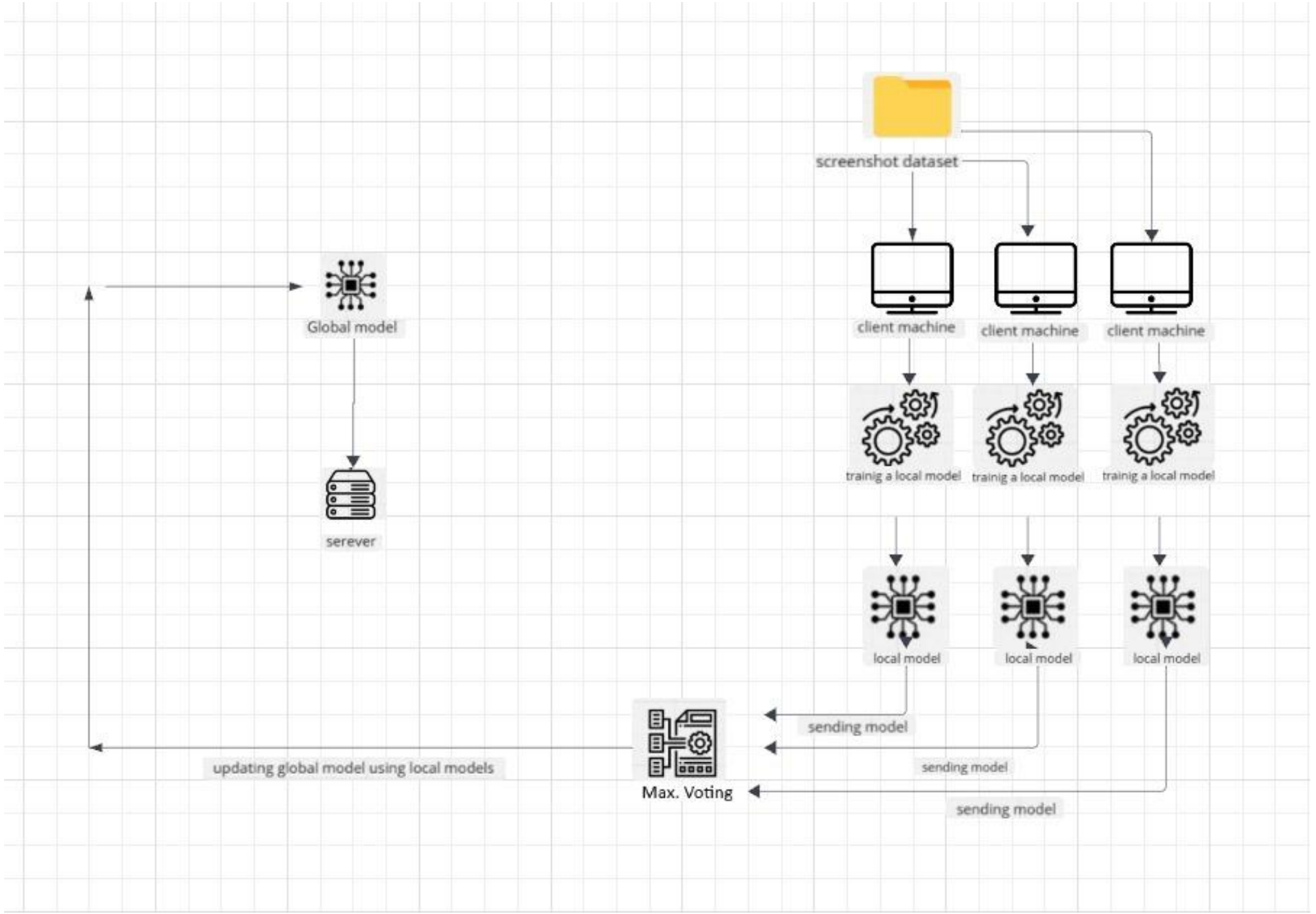
- In federated learning, the data remains on the individual devices or servers that generate it, and the model is trained on each of these decentralized data sources in a collaborative manner.
- The model itself is not shared with the individual devices or servers, and only the updated model weights are transmitted back and forth between the devices and the central server.
- Importantly, the entire detection process takes place solely on the user's device, with no transmission or uploading of local data to the cloud.

# COMPARISON

| Privacy Preserving Techniques | Privacy | Utility | Accuracy | Computational Complexity |
|---|---|---|---|---|
| Differential privacy | High | Low | Low | Low |
| Homomorphic encryption | Medium | High | High | High |
| Secure multi-party computation | High | Medium | Medium | High |
| Federated learning | High | Medium | High | Low |

# METHODOLOGY OVERVIEW

- Select the best model for classification according to the dataset.
- Set up Local and Global Model.
- The YouTube Extension will silently take a screenshot of the entire screen once every minute and send it to Local Model for classification.
- The screenshot will be analyzed by the local model and classify the image.
- Another YouTube extension saves images in respective folders of class- productive or unproductive.
- Update Global Model using Local Model weights.
- Weights are used to update the server, hence privacy is maintained.
- Every client will give binary classification and on basis of result of max voting, global model is updated.


screenshot dataset
client machine
client machine
client machine
trainig a local model
trainig a local model
trainig a local model
local model
local model
local model
sending model
sending model
sending model
Max. Voting
updating global model using local models
Global model
serever

# FEDERATED LEARNING IN OUR PROJECT

- We have created a Global Model and Local Model on the basis of comparison between various CNN models.
- Local model does the classification on the client's PC and saves the result in their respective files.
- Only the weights achieved after classification in local model are sent to Global model.
- Global model is updated.
- Hence, user privacy is preserved.

# DATASET CREATION

- We have taken around 2700 screenshots of different YouTube channels.
- Productive images: 1512
- Unproductive images: 1181
- After pre-processing of these images, the three models – simple CNN, InceptionV3, InceptionResNetV2 are trained and validated.

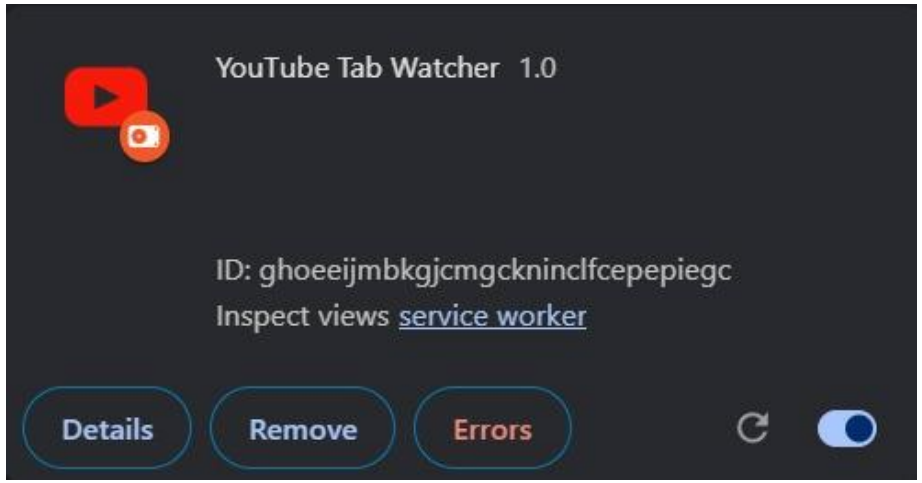
# MODEL EVALUATION

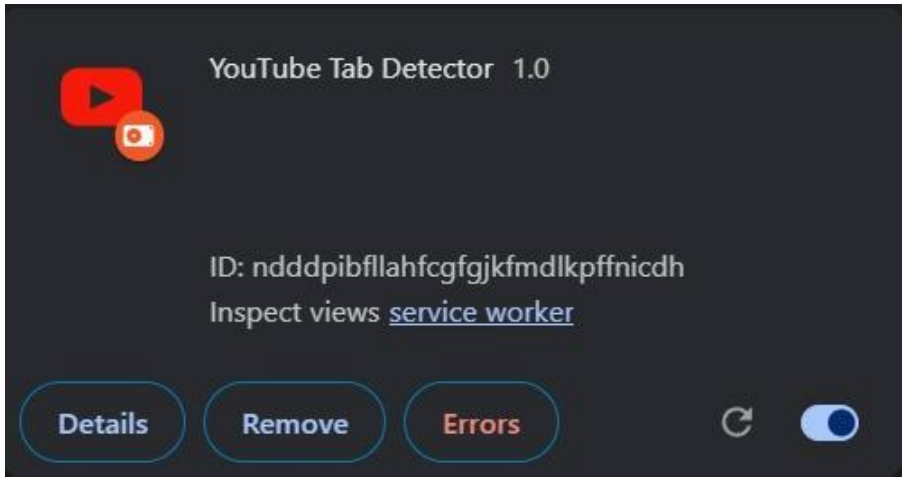
- We have taken three models- simple CNN, InceptionV3, InceptionResNetV2.
- To access the performance of our model, we have used various evaluation metrices like accuracy, precision, recall, AUC, PRC.
- Based on their performance, the best model came out to be InceptionV3.

| Models | Accuracy | Precision | Recall | AUC | PRC |
|---|---|---|---|---|---|
| InceptionV3 | 0.987 | 1.0 | 0.9705 | 0.9997 | 0.9996 |
| CNN | 100 | 100 | 100 | 100 | 100 |
| InceotionResNetV2 | 0.9833 | 0.9914 | 0.9705 | 0.9979 | 0.9974 |

# EXTENSIONS

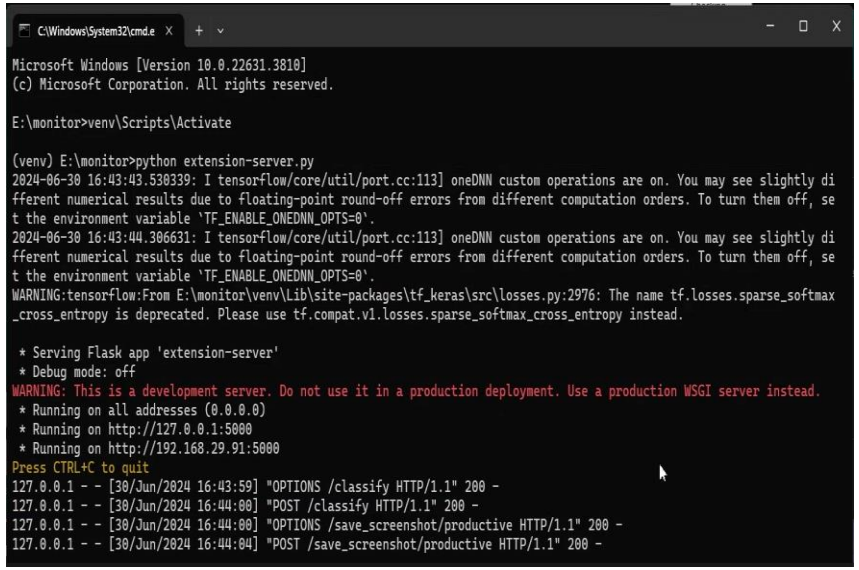
- We have created two YouTube Tab extension- YouTube Tab Watcher, YouTube Tab Detector.
- YouTube Tab Watcher classifies the screenshot as productive or unproductive.
- YouTube Tab Detector saves the classified screenshot on client's file manager.

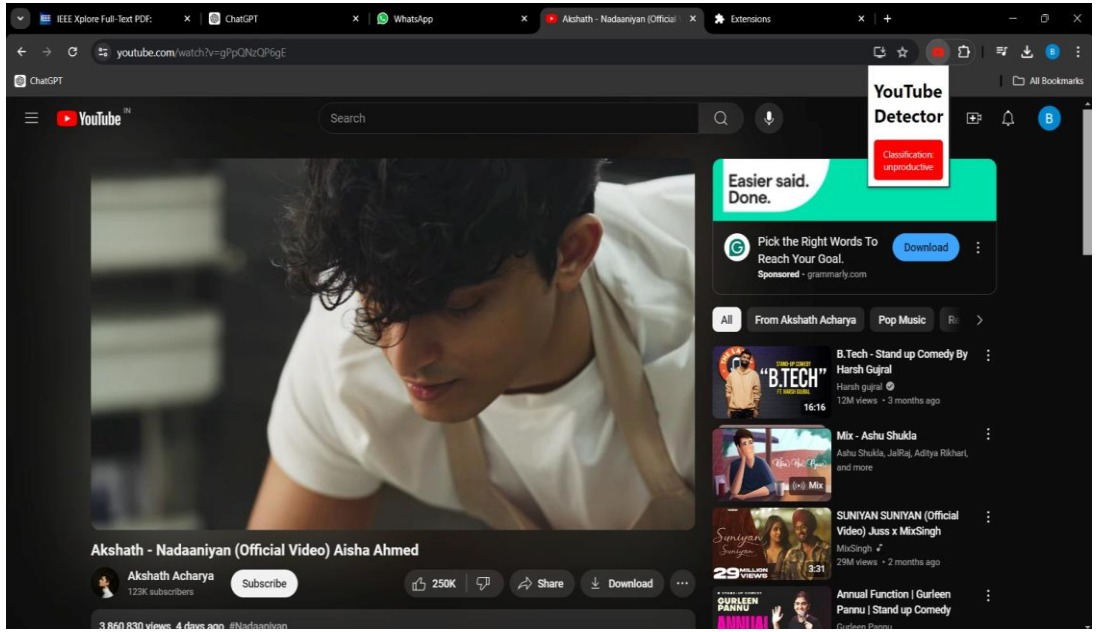


# CLASSIFICATION

- We have created a copy of Global model on client side (local model).
- YouTube Tab Watcher detects whether the screenshot taken by Local model is productive or unproductive.

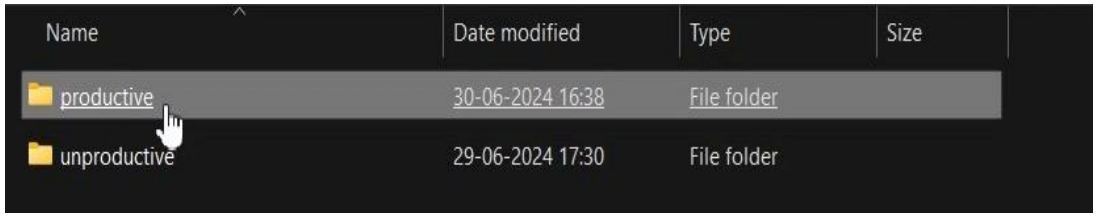


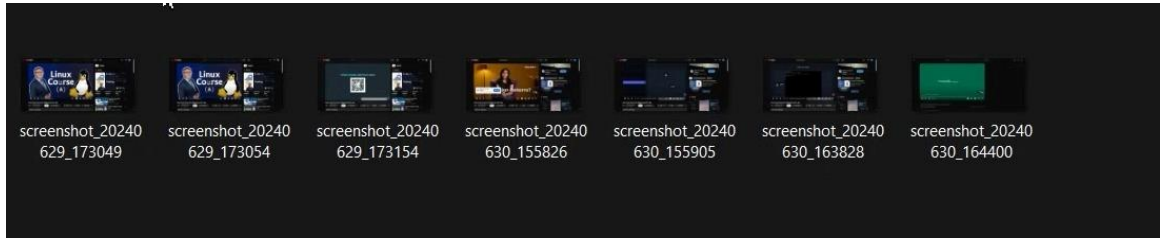



# FOLDER CREATION

- After taking the screenshot every minute, a folder named ’screenshot’ is created in file manager by the extension YouTube tab detector.

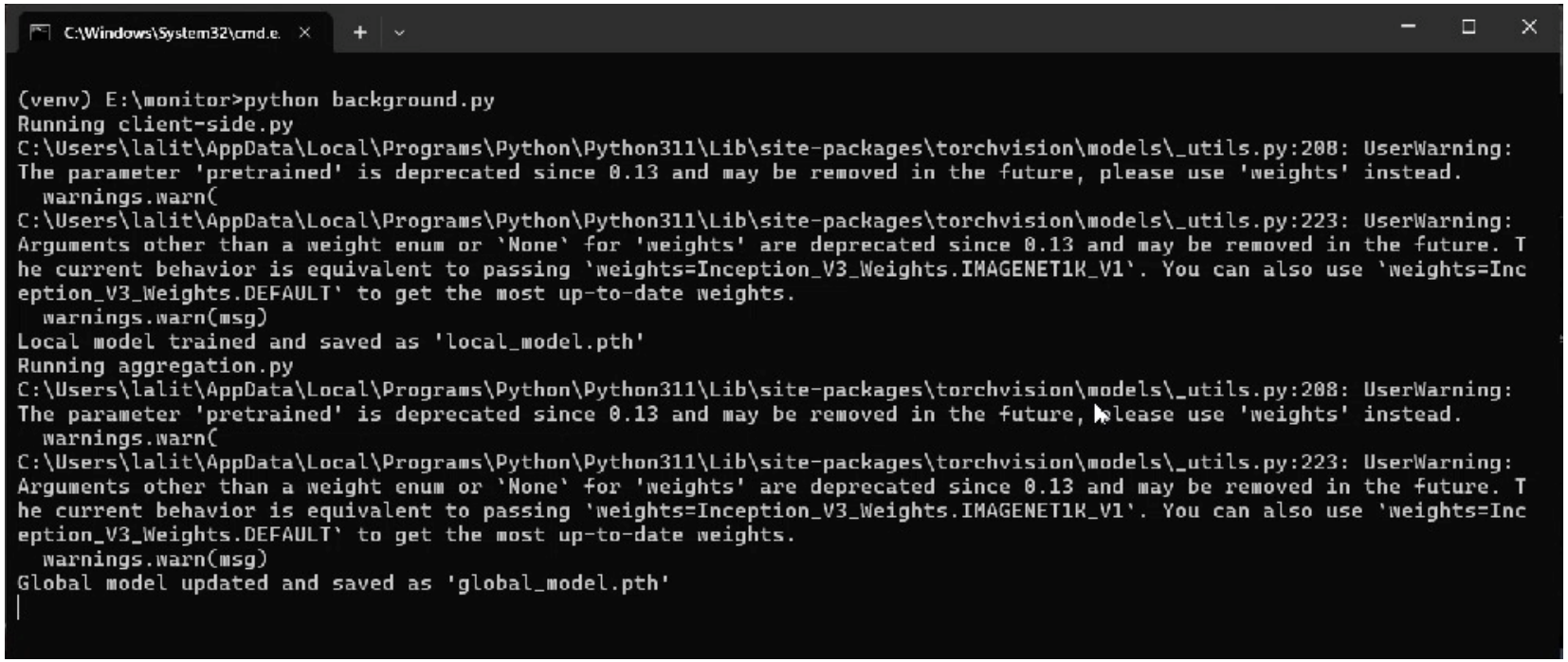

- YouTube extension classifies the screenshot as productive or unproductive and save it in their respective folders.



# UPDATE GLOBAL MODEL

- In the background, the Client model and Global model run simultaneously at one-minute intervals. After the screenshot is taken, the Client model updates its weight to Global model. Update Global model by using simple voting from the weights achieved from various local models.



# CONCLUSION

- Our project achieved classification using InceptionV3.
- Utilized Federated Learning to ensure user data remains private and secure by enabling decentralized model training on local devices, mitigating privacy risks associated with centralized data storage.
- Overall, our project exemplifies the synergy between advanced machine learning methodologies and privacy-preserving technologies, offering a compelling framework for enhancing user interaction and security in digital environment.

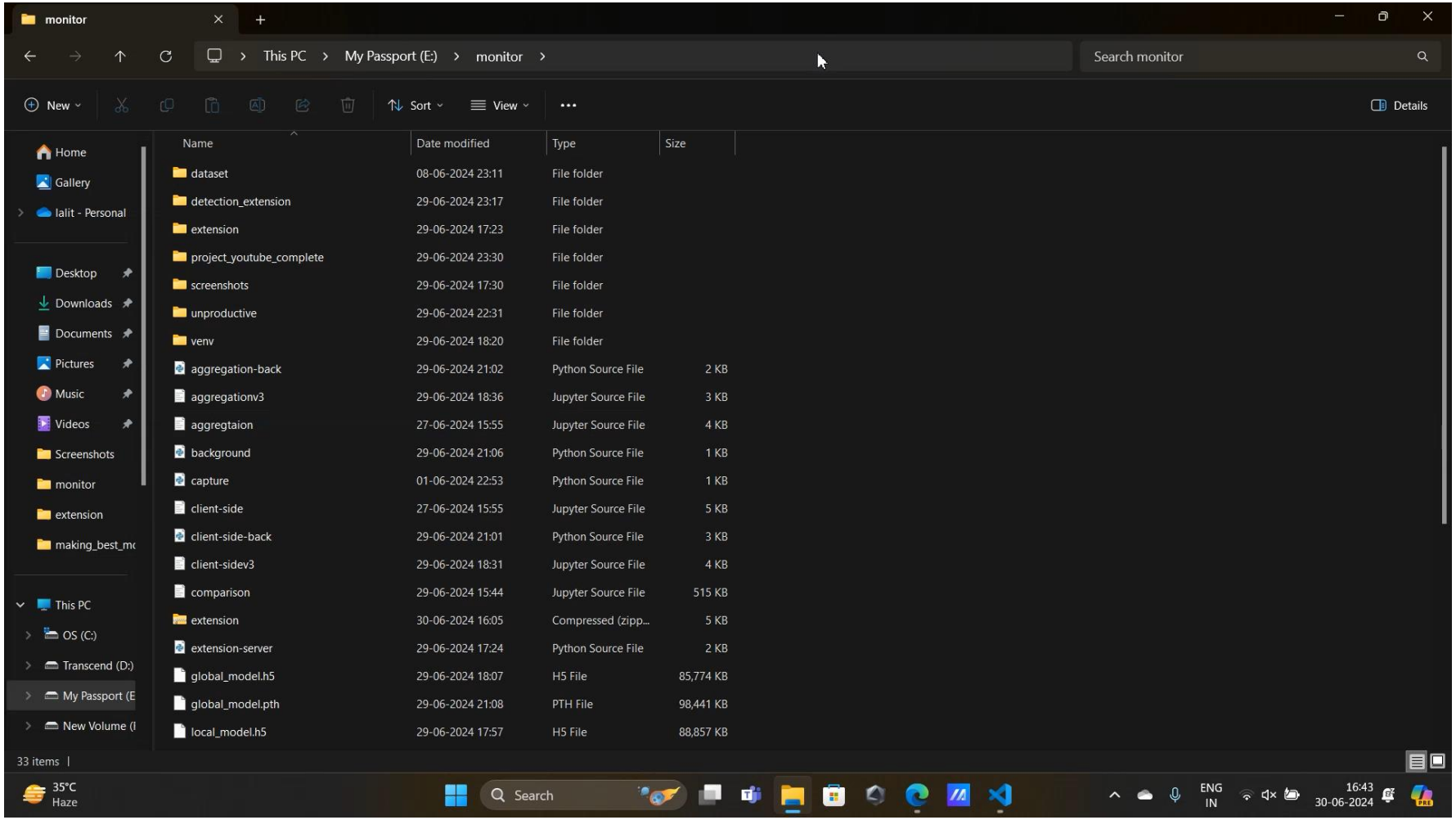
# FUTURE WORK

- Increase the size of dataset to make the model work more accurately.
- Make use of the achieved classification to make conclusions about the user.
- Accomodate screens of various devices to enhance its applicability in the real-world.

# REFERENCES


- N. Hasan B. J. Ferdosi, M. Sadi and M. A. Rahman. Tracking digital device utilization from screenshot analysis using deep learning.
- https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10196311. ‘consumption of social media and academic performance: A cross-sectional survey of perception of students in kp universities.
- B. Imler and M. Eichelberger. Using screen capture to study user research behavior
- J.Goet. ‘impact of social media on academic performance of students
- P. Krieter and A. Breiter. Track every move of your students: Log files for learning analytics from mobile screen recordings.
- H. S. Ullah S. I. U. Rehman and A. Akhtar. ‘consumption of social media and academic performance: A cross-sectional survey of perception of students in kp universities.

# PRACTICAL IMPLEMENTATION



# THANK YOU