A MAJOR PROJECT REPORT

ON

FILE ACCESS CONTROL FOR MULTIPLE USERS USING CV

Submitted in partial fulfillment of the requirement

for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

(Artificial Intelligence & Machine Learning)

BY

D.Sathwik Reddy (20P61A6614)

M.Nithin Reddy (20P61A6635)

T.Nikhil (20P61A6650)

Under the esteemed guidance of

Mrs.P.Navya

Assistant Professor

Counselling Code : VBIT

VIGNANA BHARATHI
Institute of Technology ®

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

Counselling Code : VBIT

VIGNANA BHARATHI
Institute of Technology

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

Aushapur(V), Ghatkesar(M), Hyderabad, Medchal – Dist, Telangana – 501 301.

DEPARTMENT

OF

COMPUTER SCIENCE & ENGINEERING

(Artificial Intelligence & Machine Learning)

CERTIFICATE

*This is to certify that the major project titled "**File Access control For Multiple Users Using CV**" submitted **by D.Sathwik Reddy(20P61A6614), M.Nithin Reddy(20P61A6614), T.Nikhil(20P61A6650)** in B.Tech IV-II semester Computer Science & Engineering(Artificial Intelligence & Machine Learning) is a record of the bonafide work carried out by them.*

The results embodied in this report have not been submitted to any other University for the award of any degree.

INTERNAL GUIDE **Mrs. P. Navya**	**PROJECT CO-ORDINATOR** **Mrs. P. Navya**
HEAD OF THE DEPARTMENT **Dr. K. Shirisha Reddy**	**EXTERNAL EXAMINER**

DECLARATION

We**, D.Sathwik Reddy, M.Nithin Reddy, T.Nikhil,** bearing hall ticket numbers **20P61A6614, 20P61A6635, 20P61A6650** hereby declare that the major project **“File Access Control For Multiple User Using CV”** under the guidance of **Mrs. P. Navya,** Department of Computer Science Engineering(Artificial Intelligence & Machine Learning), **Vignana Bharathi Institute of Technology, Hyderabad,** have submitted to Jawaharlal Nehru Technological University Hyderabad, Kukatpally, in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Artificial Intelligence & Machine Learning).

This is a record of bonafide work carried out by us and the results embodied in this project have not been reproduced or copied from any source. The results embodied in this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

D.Sathwik Reddy (20P61A6614)
M.Nithin reddy (20P61A6635)
T.Nikhil (20P61A6650)

ACKNOWLEDGEMENT

We are extremely thankful to our beloved Chairman, **Dr.N.Goutham Rao** and Secretary, **DR.G. Manohar Reddy** who took keen interest to provide us the infrastructural facilities for carrying out the project work. Self-confidence, hard work, commitment and planning are essential to carry out any task. Possessing these qualities is sheer waste, if an opportunity does not exist. So, we whole heartedly thank **Dr. P. V. S. Srinivas**, Principal, and **Dr. K. Shirisha Reddy**, Head of the Department, Computer Science and Engineering (Artificial Intelligence & Machine Learning) for their encouragement and support and guidance in carrying out the project.

We would like to express our indebtedness to the project coordinator, **Mrs. P. Navya**, Assistant Professor, Department of CSE (Artificial Intelligence & Machine Learning) for her valuable guidance during project work.

We thank our Project Guide, **Mrs. P. Navya**, for providing us with an excellent project and guiding us in completing our major project successfully.

We would like to express our sincere thanks to all the staff of Computer Science and Engineering (Artificial Intelligence & Machine Learning), VBIT, for their kind cooperation and timely help during our project. Finally, we would like to thank our parents and friends who have always stood by us whenever we needed them.

ABSTRACT

In recent years, the ubiquity of facial detection software, exemplified by technologies like Windows Face ID, Apple Face ID, and smartphone face unlock, has significantly elevated the standards of data security and access control. While these advancements have been pivotal in individualized device authentication, challenges arise when multiple users share a system, necessitating tailored solutions to safeguard private files and personalized data. In response to this, our paper proposes an innovative model that seamlessly integrates three key components. The first component involves precise Facial Recognition, leveraging unique facial features for individual user identification, thereby ensuring that access is limited to authorized individuals, whether unlocking a smartphone or accessing sensitive files. The second component, File and App Locking, addresses the paramount concern of privacy in shared systems, allowing users to protect specific files and applications, thereby thwarting unauthorized access and preserving confidentiality in communal settings. Finally, Basic Image Processing serves as the third component, playing a pivotal role in enhancing overall system accuracy and security. This step fine-tunes facial recognition algorithms, identifies potential vulnerabilities, and optimizes image quality by minimizing noise and improving clarity, contributing to a robust user authentication process. Through the integration of these three components, our model provides a comprehensive and adaptive solutions.

Keywords:

- Facial Recognition, File and App Locking, Basic Image Processing, Security, Privacy, Data Integrity, Authorized Users, Unauthorized Access, Personalized Security, Shared Systems.

DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING

(Artificial Intelligence & Machine Learning)

VISION

To achieve global standards of quality in technical education with the help of advanced resources and automated tools to bridge the gap between industry and academia.

MISSION

- Build the students technically competent on global arena through effective teaching learning process and world-class infrastructure.
- Inculcate professional ethics, societal concerns, technical skills and life-long learning to succeed in multidisciplinary fields.
- Establish competency centre in the field of Artificial Intelligence and Machine Learning with the collaboration of industry and innovative research.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

PEO 1: Domain Knowledge: Impart strong foundation in basic sciences, Mathematics, Engineering and emerging areas by Advanced tools and Technologies.

PEO 2: Professional Employment: Develop Professional skills that prepare them for immediate employment in industry, government, entrepreneurship and R&D.

PEO 3: Higher Degrees: Motivation to pursue higher studies and acquire masters and research.

PEO 4: Engineering Citizenship: Communicate and work effectively, engage in team work, achieve professional advancement, exhibit leadership skills, and ethical attitude with a sense of social responsibility.

PEO 5: Lifelong Learning: Lead edge of the industrial engineering discipline and respond to challenges of an ever-changing environment with the most current knowledge and technology.

PROGRAM OUTCOMES (POs)

Engineering graduates will be able to:

1. **Engineering Knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem Analysis**: Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, and environmental considerations.

4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society**: Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues, and the consequent responsibilities relevant to professional engineering practice.

7. **Environment and sustainability**: Understand the impact of professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.

9. **Individual and teamwork**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective Presentations, and give and receive clear instructions.

11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary Environments.

12. **Life-long learning**: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs)

PSO1: Understand and Apply Multi-Disciplinary and core concepts with emerging technologies for sustaining with the Dynamic Industry Challenges.

PSO2: Design Automated Applications in Machine Learning, Deep Learning, Natural Language Processing and Relevant Emerging areas for visualizing, interpreting the datasets.

PSO3: Develop Computational Knowledge, project and Interpersonal skills using innovative tools for finding an elucidated solution of the real-world problems and societal needs.

Course Outcomes (COs)

CO1 - Identify the problem by applying acquired knowledge from survey of technical publications.

CO2 - Analyze and categorize identified problem to formulate and fine the best solution after considering risks.

CO3 - Choose efficient tools for designing project.

CO4 - Build the project through effective teamwork by using recent technologies.

CO5 - Elaborate and test the completed task and compile the project report.

Correlation Levels

Substantial/High	3
Moderate Medium	2
Slight/Low	1
No correlation	

CO-PSO Correlation Matrix

COs	PSOs		
	PSO1	PSO2	PSO3
CO1	2	1	3
CO2	3	2	2
CO3	1	3	
CO4	2	1	3
CO5		2	1
CO	1.6	1.8	1.8

CO-PO Correlation Matrix

COs	POs											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3		3	3	3	3	2	2	2	2	2	3
CO2	2	3	1		2		2	3	3	3	3	2
CO3		2	2	3	1	2		2	2	2	2	1
CO4	2	3	3		2	3	3	3	3	3	3	2
CO5	3	1	2	3			1		1	2	2	2
CO	2	1.8	2.2	1.5	1	1.6	1.7	2.2	2.2	2.4	2.4	2

Project Outcomes (PROs)

1. **File access control** : The project ensures the security of necessary files. It works for a single user system with multiple administrators and different assigned files. It restricts file access by hiding the files.
2. **Second step verification :** In case of face recognition failure or unknown user detection, the project gives a second attempt by asking a security question.

3. **Forced sleep mode:** Failure of second step verification will be considered as security breach. This results the pc to go into the sleep mode.
4. **Improved security by database:** In case of security breach, The code stores the images of unknown users and saves in the database allowing the legal administrators to check and verify.
5. **Automated mail (optional):** The pictures that are saved in the database can be automatically sent to an email of administrator.

PRO-PSO Correlation Matrix

PROs	**PSOs**		
	PSO1	**PSO2**	**PSO3**
PRO1	3	2	1
PRO2	2	3	2
PRO3	1	2	3
PRO4	2	1	2
PRO5	1	2	3
PRO	1.8	2	2.2

PRO – PO Correlation Matrix

PROs	**POs**											
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
PRO1	2	2	2	2	3	3		3	3	3	3	2
PRO2	3	3	3	3	2	2	3	1		2		2
PRO3	2	2	2	2	1		2	2	3	1	2	
PRO4	3	3	3	3	2	2	3	3		2	3	3
PRO5		1	2	2	2	3	1	2	3			1
PRO	2.2	2.2	2.4	2.4	2	2	1.8	2.2	1.5	1	1.6	1.7

TABLE OF CONTENTS

List of Figures

CHAPTER – 1

1.Introduction

In recent years, facial detection software like Windows Face ID, Apple Face ID, and smartphone face unlock have aimed to secure data and limit unauthorized access. However, challenges arise when multiple users share a system, particularly concerning private files and personalized data security. Our innovative model addresses these concerns by incorporating facial recognition, file and app locking, and basic image processing. This approach ensures individual user security in shared systems. Facial recognition accurately distinguishes users based on unique facial features, forming the foundation for personalized security measures. File and app locking lets users protect specific files and applications from unauthorized use, maintaining privacy in communal settings. Basic image processing enhances accuracy and security, identifying potential vulnerabilities .In essence, our model provides a comprehensive solution to safeguard personalized data within shared systems, offering confidence in maintaining privacy and data integration.

1. **Facial Recognition:** This cutting-edge technology analyzes unique facial features to accurately identify users. Whether it's Windows Face ID, Apple Face ID, or smartphone face unlock, facial recognition forms the bedrock of personalized security measures. By ensuring that only authorized individuals can access the system, it safeguards data and privacy.

2. **File and App Locking:** In shared systems, privacy is paramount. File and app locking empowers users to protect specific files and applications from unauthorized access. Whether it's confidential documents, personal photos, or sensitive apps, this feature ensures that each user's private data remains secure.

3. **Basic Image Processing:** Enhancing accuracy and security, basic image processing plays a crucial role. It identifies potential vulnerabilities and fine-tunes facial recognition algorithms. By optimizing image quality and minimizing noise, this step contributes to robust user authentication.

1.1 Existing System:

If we have to mention a few examples of current security applications which use face detection, the obvious mentions would be Apple Face ID, Windows Hello.

Windows Hello: Windows Hello is a built-in feature in Windows 10 that uses facial recognition (and other biometric methods) to authenticate users and unlock Windows devices. It uses infrared and depth sensors for improved security.

Apple Face ID: Apple's Face ID is a facial recognition authentication system used in iPhones and iPads. It uses a combination of infrared and visible light to map and authenticate the user's face.

To comprehensivise, the existing models provide security to a user’s data by restricting it to the non users. They use biometric methods like Finger print or Face Detection.

1.2 Proposed System:

As the introduction of the model was explained in abstract, Highlighting the key features and benefits can elaborate. The key features of the model are face detection(open cv), Access control based on recognized users for personal experience, File and app locking to restrict unauthorized access and forcing the system to sleep mode in case of access from non administrator.

The benefits include Enhanced Security(protecting the data from unauthorized access), adapting to user convenience by allowing customization of file selections that to be secured and scalability(adaptable to more than one user).

With the modification of multi user system and addition of customization feature, this can stand as unique model and help multiple users with file access control.

1.3 Aim and Objective:

The aim of the project:

The primary goal of integrating face recognition into file access control systems is to enhance security and streamline access management. By leveraging facial data, this technology aims to provide a robust and efficient method for granting or denying access to secured areas.

The objectives of this project are:

- **Enhanced Security:** Face recognition ensures that only authorized individuals can access files and sensitive data. It eliminates the need for traditional access methods like keys or cards, reducing the risk of unauthorized entry.
- **Convenience and Efficiency:** Users no longer need physical tokens (such as keys or access cards) to gain entry. Facial recognition simplifies the authentication process, making it more convenient for users.
- **Reduced Administrative Overhead:** Automated face recognition reduces administrative tasks related to managing access permissions. It streamlines user authentication, minimizing the need for manual intervention.
- **Real-time Monitoring:** The system can continuously monitor access points, detecting any unauthorized attempts. Alerts can be triggered when unrecognized faces are detected, enhancing security.
- **Integration with Existing Systems:** Implementing face recognition seamlessly integrates with existing access control infrastructure, ensuring a smooth transition and compatibility.
- **Scalability:** The system can handle a large number of users without compromising accuracy or performance.
- **Privacy Considerations:** Balancing security with privacy is crucial. Objectives include designing the system to protect user privacy while maintaining effective security measures.

1.4 Scope:

User Authentication and Authorization:

Scope: The system aims to authenticate users based on their facial features.

Access Control Policies:

Scope: Defining rules for access permissions.

Integration with Existing Systems:

Scope: Ensuring seamless integration.

Privacy and Data Protection:

Scope: Balancing security with privacy.

Monitoring and Auditing:

Scope: Real-time surveillance and audit trails.

Performance and Scalability:

Scope: Efficient processing for large user bases.

User Experience and Usability**:**

Scope: Ensuring a seamless user journey.

CHAPTER – 2

2.Literature Survey

1. “Data Hiding Techniques Using Steganography Algorithms” [1] by (Rahul Veer Singh's.,2020)

The research of Ashi, Rahul and srishti on data hiding techniques using steganography highlighted future scope in the area. It explores the basic principles of steganography, emphasizing the delicate trade-off that the method's intrinsic security and capacity must make. It presents ideas intended to reduce the chance of steganalysis detection while simultaneously improving security and capacity. The conversation continues by examining image steganography, which is a widely used and complex technique for data concealing. It emphasizes how simple this technique is—only the sender and recipient are aware of it. The idea of maintaining image integrity by locating areas with the least amount of distortion lies at the heart of this technique.

2. “File access destination control device and method” [2] by (Takahisa Shirakawa.,July 2003)

The study by Takashi on file access destination has brought to light disparities in national laws concerning the GDPR's application to the processing of personal data for scientific purposes. These differences could impair data subject protection standards, impede information interchange, and produce legal ambiguities. While it is stressed how important it is to notify data subjects, there have been criticisms of several GDPR rules, including those found in Articles 13 and 14. Particular weaknesses include a lack of instructions regarding the rights of data subjects and how to get in touch with supervisory authorities.

3. "Development Of Security Systems Using Facial Recognition” [3] by (Rana Hamid.,2008)

Hamid explains security, as a state of being saved and protected, is explored in this paper. The focus lies on leveraging two emerging artificial intelligence technologies: Facial Recognition and Artificial Neural Networks. These technologies are employed to develop secure keyless door networks, where only authorized faces can open the door. The system includes a camera-equipped door interface with a PC for capturing and processing images. The introduction highlights the evolution of security concepts, considering viewpoints from various angles, including those of terrorist organizations. Enhanced security measures evoke feelings of happiness and peace of mind. And the authors felt that their model could be improved with independency of MATLAB.

4. "Smart Lock Systems: An Overview" [4] by (Diamond Celestine aluri., 2020):

The smart lock, a modern successor to traditional locks, is the focus of this paper. It provides an overview of various smart lock technologies. The smart lock system, now widely adopted in homes and commercial buildings, offers user-friendly benefits with manageable downsides.

Technology has significantly impacted our lives, including the Home Automation System—a computerized network controlling electronic devices and monitoring home appliances efficiently. Among emerging real-time applications, the Home Security System stands out. The smart lock system gradually replaces traditional locks due to its convenience and affordability. Smart locks operate wirelessly using cryptographic keys, granting access only to authorized personnel. Biometric systems (such as fingerprint recognition) enhance security. Some smart locks even incorporate cameras. Smart locks play a crucial role in smart connected homes, serving both commercial and residential security needs. They allow third-party access via virtual keys sent to recipients' smartphones through Wi-Fi, mobile apps, proximity sensors, and Bluetooth Low Energy (BLE).

5."Control of Access to Files” [5] by (Arun Balasubramanyam et al., 2012):

Embodiments of the present invention involve a method, system, and program product for using access-control lists (ACLs) to control access to computer files. These embodiments receive and store classifications of two or more computer files where those classifications fall within a single category. The category may identify products, product lines, geographic locations, customer account identifiers, network types, server platform types, or server operating statuses associated with an access-controlled file. The method checks the access-control list in response to a user's request for access to determine if the user is authorized.

In Summary, Research papers cover steganography principles, emphasizing security and capacity trade-offs. Image steganography conceals data within images, focusing on maintaining image integrity. Another paper discusses GDPR implications on personal data processing, highlighting disparities in national laws. Facial recognition and artificial neural networks are explored for secure keyless door systems. Smart lock systems offer convenience and security, replacing traditional locks in homes and commercial buildings. Access-control lists are utilized to manage access to computer files based on classifications.

CHAPTER - 3

3.Design

3.1 Hardware Requirements:

1) PC or Workstation:

- PC with a modern operating system (Windows 7 or higher, or Linux).
- Compatibility with TensorFlow and MIDI processing libraries

2) Processor:

- A multi-core processor (quad-core or higher) for faster training.
- Modern processors like Intel Core i5/i7 or AMD Ryzen series are recommended.

3) RAM (Random Access Memory):

- 8 GB or higher for efficient model training.
- Face Recognition using computer vision, can benefit from larger RAM.

4) Storage:

- At least 20 GB of free disk space for storing datasets, model checkpoints, and logs.
- SSD (Solid State Drive) is preferred for faster data access.

5) GPU (Optional but Recommended):

- A dedicated GPU, such as NVIDIA GeForce or Quadro series, is highly recommended.
- For more substantial projects, consider using NVIDIA GPUs like GTX 10 series, RTX 20 series, or higher.

6) Internet Connection:

- A stable internet connection for downloading libraries, dependencies, and potential model weights.
- Useful for collaborative work, accessing resources, and staying updated with the latest tools.

7) Jetson Nano Board (Optional):

- If we want to deploy the trained model on edge devices, the Jetson Nano board could be considered.
- This is optional for training but beneficial if you plan to deploy the model to resource-constrained environments.

3.2 Software Requirements:

1. Anaconda Navigator: Anaconda Navigator is used for managing Python packages and virtual environments, ensuring a consistent and compatible environment for various components of the project, such as OCR and machine learning libraries.
2. Jupyter Notebook: Jupyter Notebook provides an interactive and collaborative coding environment, allowing researchers to document, experiment, and share their code, making it an ideal tool for analyzing and processing the digitized manuscript data.
3. Python: Python is a versatile programming language with extensive libraries for image processing, machine learning, and natural language processing, making it well suited for building the recognition and conversion components of the project efficiently and effectively.
4. PyCharam : PyCharm is an integrated development environment (IDE) used for programming in Python. It provides code analysis, a graphical debugger, an integrated unit tester, integration with version control systems, and supports web development with Django. PyCharm is developed by the Czech company JetBrains.

3.3 Model Architecture:

The first step is to capture an image of the user's face. Then, the system compares the captured image to a database of known faces. If a match is found, the system proceeds to identify the user's identity. If no match is found, the system may prompt the user to enter a password or take other steps to verify their identity. The photos of unrecognised users will be saved in database and can be sent to mails of admin.

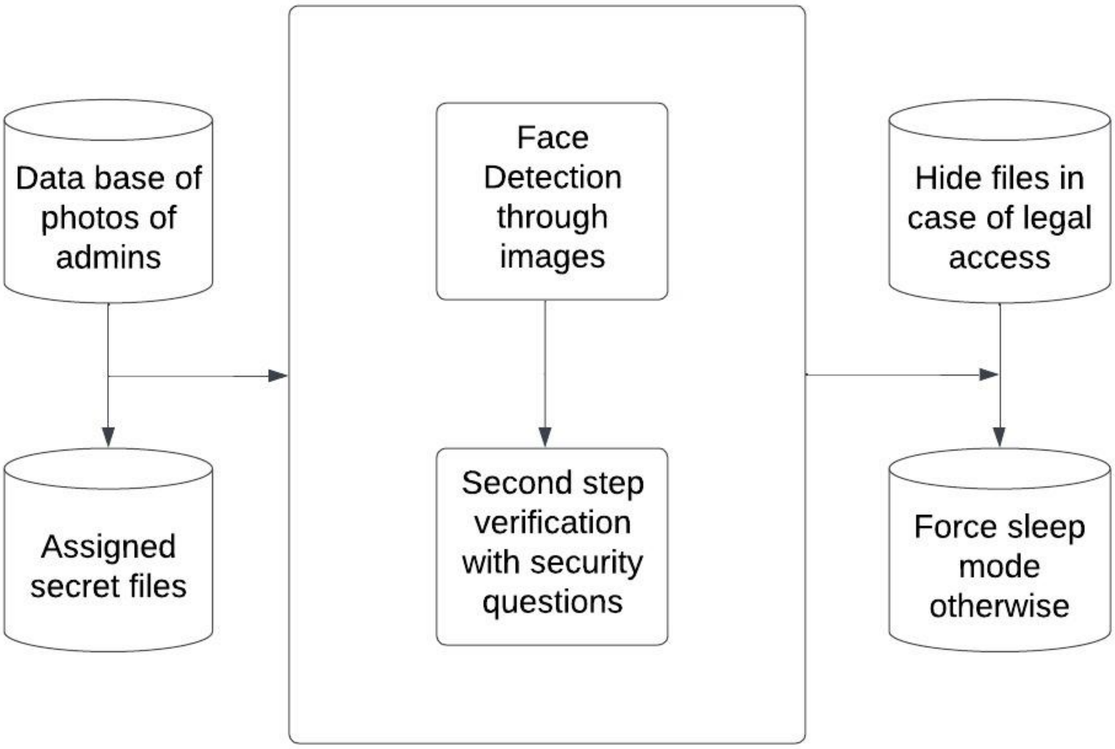

Data base of photos of admins
Assigned secret files
Face Detection through images
Second step verification with security questions
Hide files in case of legal access
Force sleep mode otherwise

Fig 1: System Architecture

3.4 Algorithms:

Face_recognition:

•Face recognition is the process or the method of recognizing faces based on their photos and videos and these systems are widely used in especially for law enforcement and caps.

•The library uses many built-in libraries such as Dlib and it uses machine learning to recognize the faces with an accuracy of 99.38% which is insane and performs better than the human brain can do

3.5 Libraries:

1) Cv2:

- The cv2 library contains over 2500 algorithms and functions for various tasks such as image processing, video analysis, object detection, face recognition, and more12.
- The cv2 library can be installed using pip, and there are different packages available depending on the environment and the modules needed1. For example, opencv-python is the main package that contains the core functionality, while opencv-contrib-python includes additional modules such as CUDA support1.
- The cv2 library can be imported using import cv2 and then used to access the OpenCV functions and classes1. For example, cv2.imread can be used to read an image from a file, and cv2.imshow can be used to display an image in a window3

2) Os:

- The os library contains methods and constants for various tasks such as file and directory handling, process management, environment variables, input and output, and more.
- The os library can be installed using pip, and it is compatible with Python 3 and supports multiple platforms such as Windows, Linux, and macOS.
- The os library can be imported using import os and then used to access the OpenCV functions and classes. For example, os.getcwd can be used to get the current working directory, and os.mkdir can be used to create a new directory.

3) Ctypes :

- The ctypes library can be installed using pip, and it supports Python 2 and 3 on Windows, Linux, and macOS.
- The ctypes library can be imported using import ctypes and then used to create and manipulate C data types, such as ctypes.c_int, ctypes.c_char, and ctypes.c_void_p.
- The ctypes library can also load dynamic libraries, such as DLLs on Windows or shared objects on Linux, using ctypes.cdll, ctypes.windll, or

ctypes.oledll. These objects can be used to access the functions and variables exported by the libraries.

3.6 Data Flow Diagram:

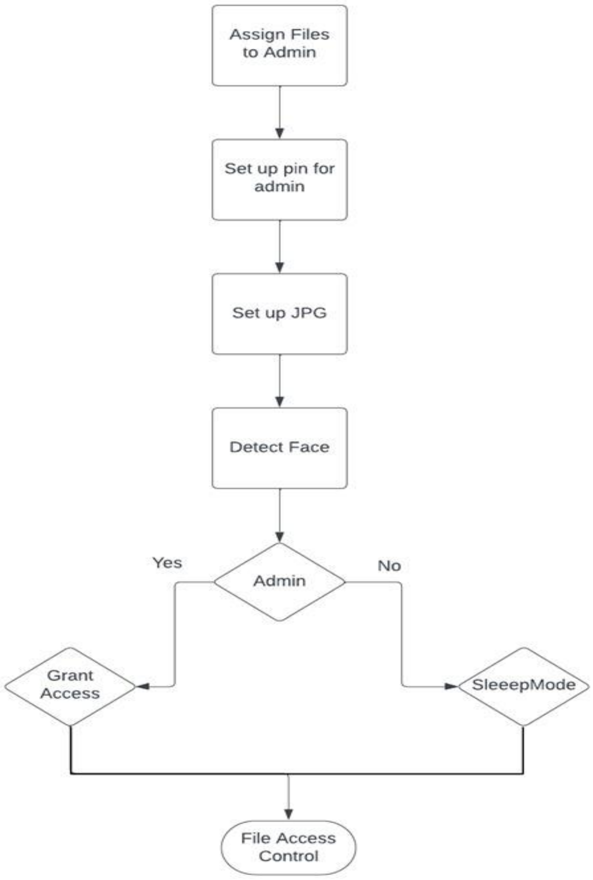
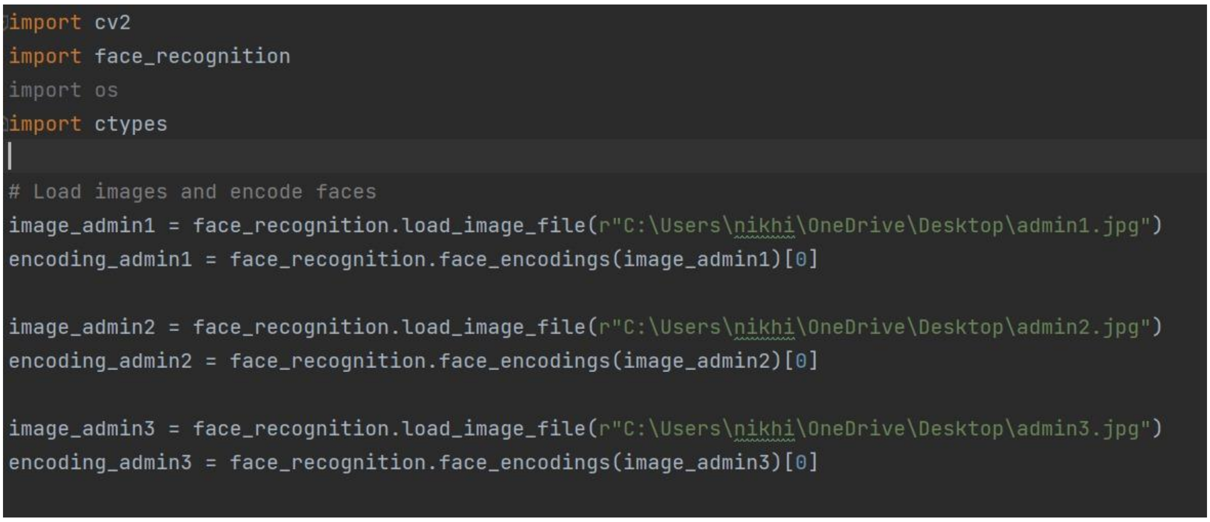


Fig 2: Data Flow Diagram

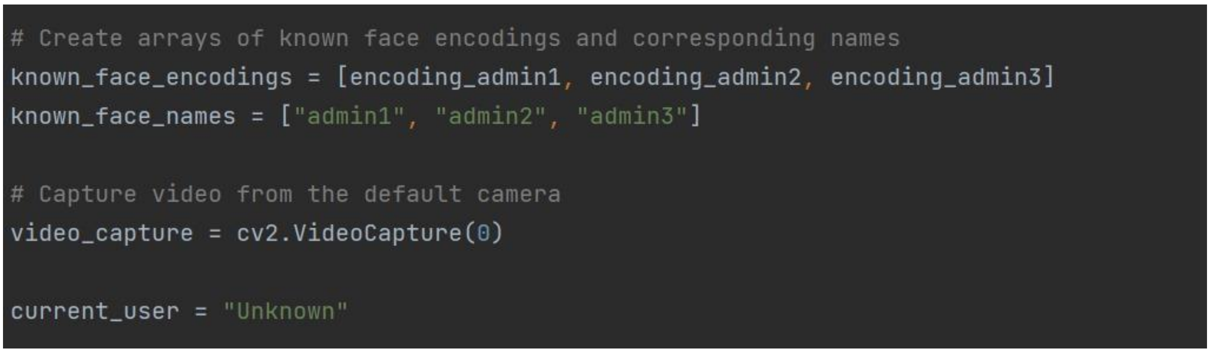
CHAPTER-4

4.Implementation:

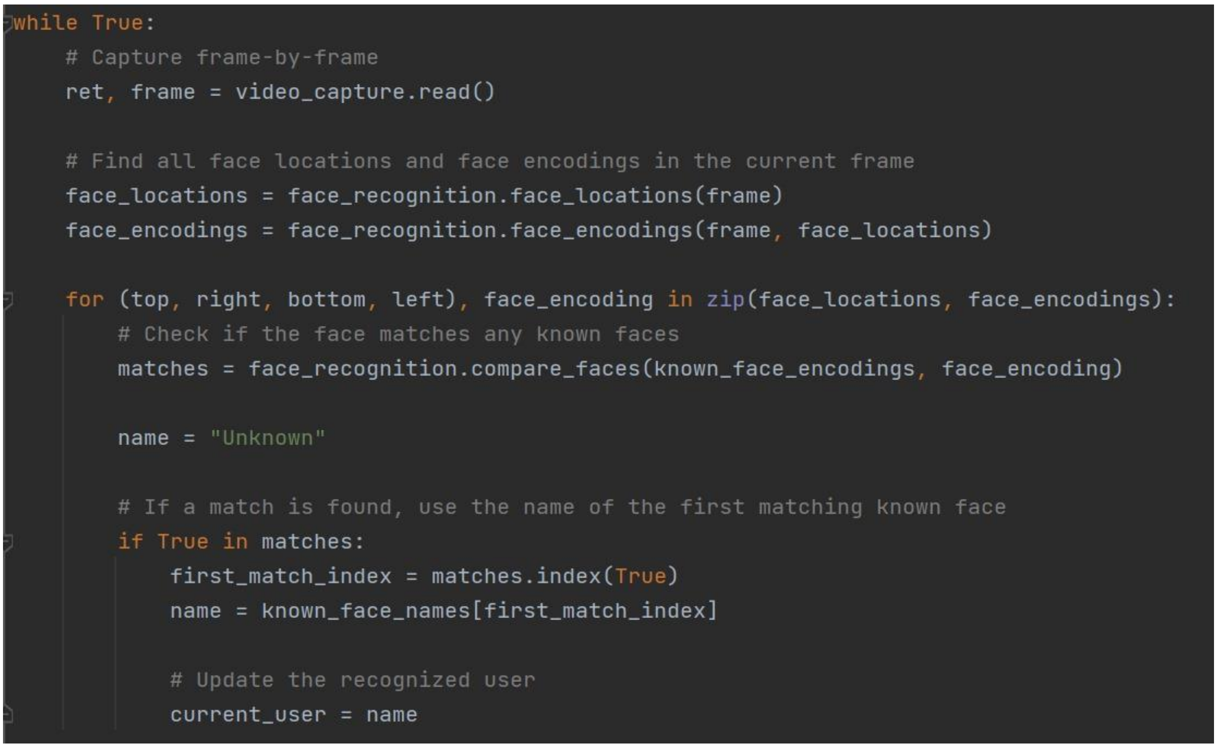
main.py



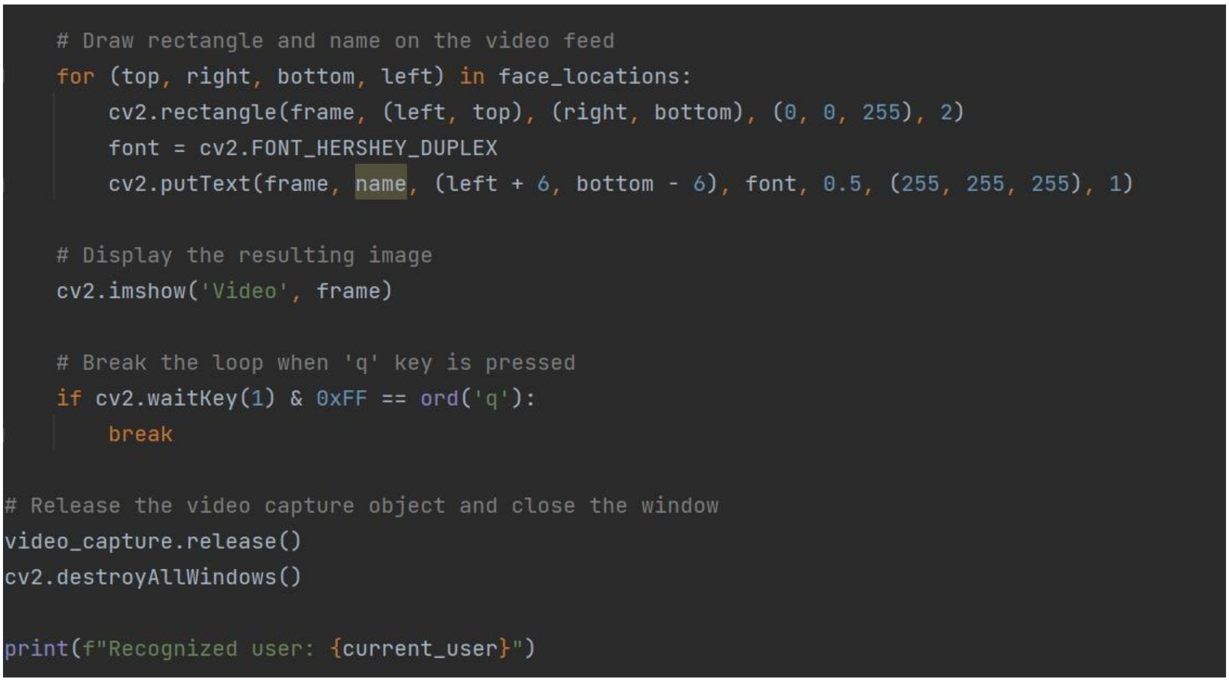
```
import cv2
import face_recognition
import os
import ctypes

# Load images and encode faces
image_admin1 = face_recognition.load_image_file(r"C:\Users\nikhi\OneDrive\Desktop\admin1.jpg")
encoding_admin1 = face_recognition.face_encodings(image_admin1)[0]

image_admin2 = face_recognition.load_image_file(r"C:\Users\nikhi\OneDrive\Desktop\admin2.jpg")
encoding_admin2 = face_recognition.face_encodings(image_admin2)[0]

image_admin3 = face_recognition.load_image_file(r"C:\Users\nikhi\OneDrive\Desktop\admin3.jpg")
encoding_admin3 = face_recognition.face_encodings(image_admin3)[0]
```



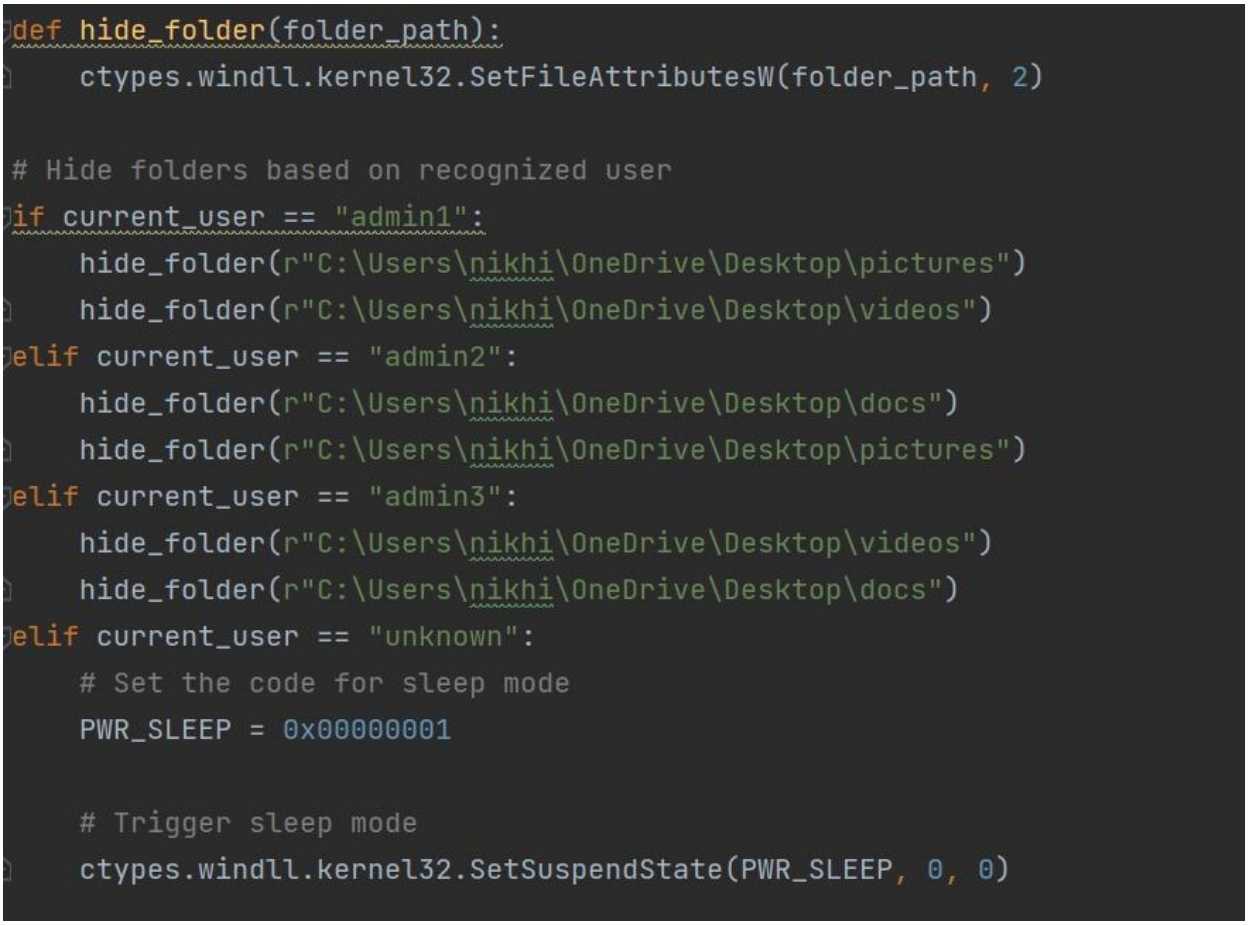
```
# Create arrays of known face encodings and corresponding names
known_face_encodings = [encoding_admin1, encoding_admin2, encoding_admin3]
known_face_names = ["admin1", "admin2", "admin3"]

# Capture video from the default camera
video_capture = cv2.VideoCapture(0)

current_user = "Unknown"
```



```python
while True:
    # Capture frame-by-frame
    ret, frame = video_capture.read()

    # Find all face locations and face encodings in the current frame
    face_locations = face_recognition.face_locations(frame)
    face_encodings = face_recognition.face_encodings(frame, face_locations)

    for (top, right, bottom, left), face_encoding in zip(face_locations, face_encodings):
        # Check if the face matches any known faces
        matches = face_recognition.compare_faces(known_face_encodings, face_encoding)

        name = "Unknown"

        # If a match is found, use the name of the first matching known face
        if True in matches:
            first_match_index = matches.index(True)
            name = known_face_names[first_match_index]

            # Update the recognized user
            current_user = name
```

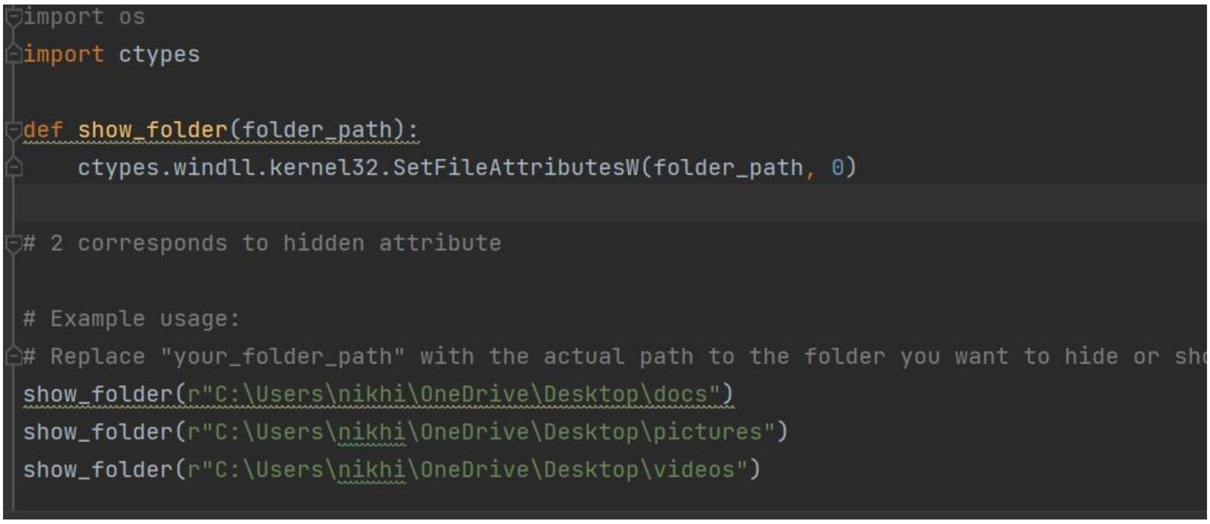


```python
    # Draw rectangle and name on the video feed
    for (top, right, bottom, left) in face_locations:
        cv2.rectangle(frame, (left, top), (right, bottom), (0, 0, 255), 2)
        font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, bottom - 6), font, 0.5, (255, 255, 255), 1)

    # Display the resulting image
    cv2.imshow('Video', frame)

    # Break the loop when 'q' key is pressed
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break

# Release the video capture object and close the window
video_capture.release()
cv2.destroyAllWindows()

print(f"Recognized user: {current_user}")
```



```
def hide_folder(folder_path):
    ctypes.windll.kernel32.SetFileAttributesW(folder_path, 2)

# Hide folders based on recognized user
if current_user == "admin1":
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\pictures")
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\videos")
elif current_user == "admin2":
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\docs")
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\pictures")
elif current_user == "admin3":
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\videos")
    hide_folder(r"C:\Users\nikhi\OneDrive\Desktop\docs")
elif current_user == "unknown":
    # Set the code for sleep mode
    PWR_SLEEP = 0x00000001

    # Trigger sleep mode
    ctypes.windll.kernel32.SetSuspendState(PWR_SLEEP, 0, 0)
```

To Reappear the Files :



```
import os
import ctypes

def show_folder(folder_path):
    ctypes.windll.kernel32.SetFileAttributesW(folder_path, 0)

# 2 corresponds to hidden attribute

# Example usage:
# Replace "your_folder_path" with the actual path to the folder you want to hide or sh
show_folder(r"C:\Users\nikhi\OneDrive\Desktop\docs")
show_folder(r"C:\Users\nikhi\OneDrive\Desktop\pictures")
show_folder(r"C:\Users\nikhi\OneDrive\Desktop\videos")
```

(refer to sample copy)

Here’s an overview of the code:

1. **Imports:** The code imports necessary Python libraries and modules for different functionalities, such as cv2 for face recognition and os for automation in background.

2. **Initialization:** It initializes face recognition to detect admins and unknown users, forms a square around the face and labels the admin.

3. **Functions:**
   - Face recognition: Recognizes the faces of admins, labels them and detects unknown user
   - Hide Files: Upon face recognition, grants access to pc and hides specific unassigned files.
   - second step verification: In case of unknown users, asks a security question to bypass.
   - Sleep mode: Forces pc to sleep mode after verification failure.

4. **Model Architecture:** Defines the architecture of the File access control using computer vision and face recognition

5. **Training the Model**: Code snippets for running face recognition, labeling the admins and hiding files.
6. **File access control:** Unassigned files of the user will be hidden and forces sleep mode in case of security breach.

7. **Saving photos of unknown users:** photos of unknown users will be saved for cross checking purposes and to enhance security.

8. **User Interface (Optional):** The code makes use of PyCharm environment and command prompt to run. It opens up a 'video' window for face recognition.

The file access control using computer vision solves the security issue of secret files in a single user system where there can be multiple admins. And also makes the pc not accessible to unknown users by forcing the sleep mode. It utilizes computer vision, face recognition and os to make all these possible.

CHAPTER-5

5.Results and Discussion

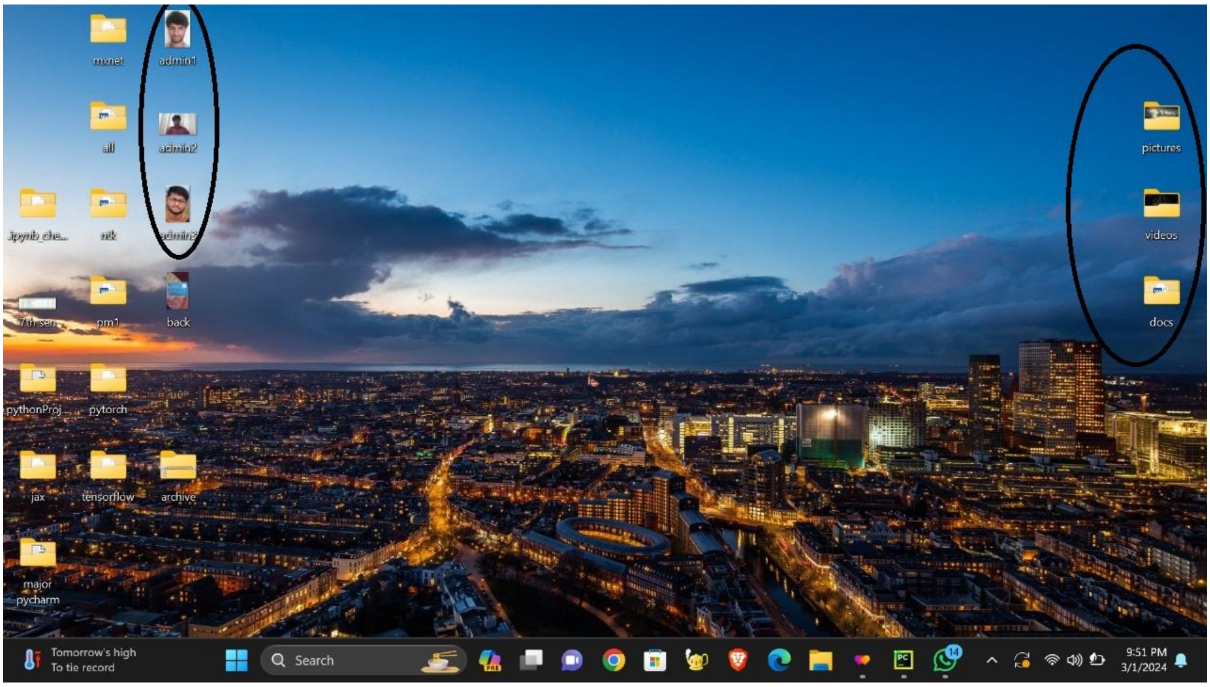
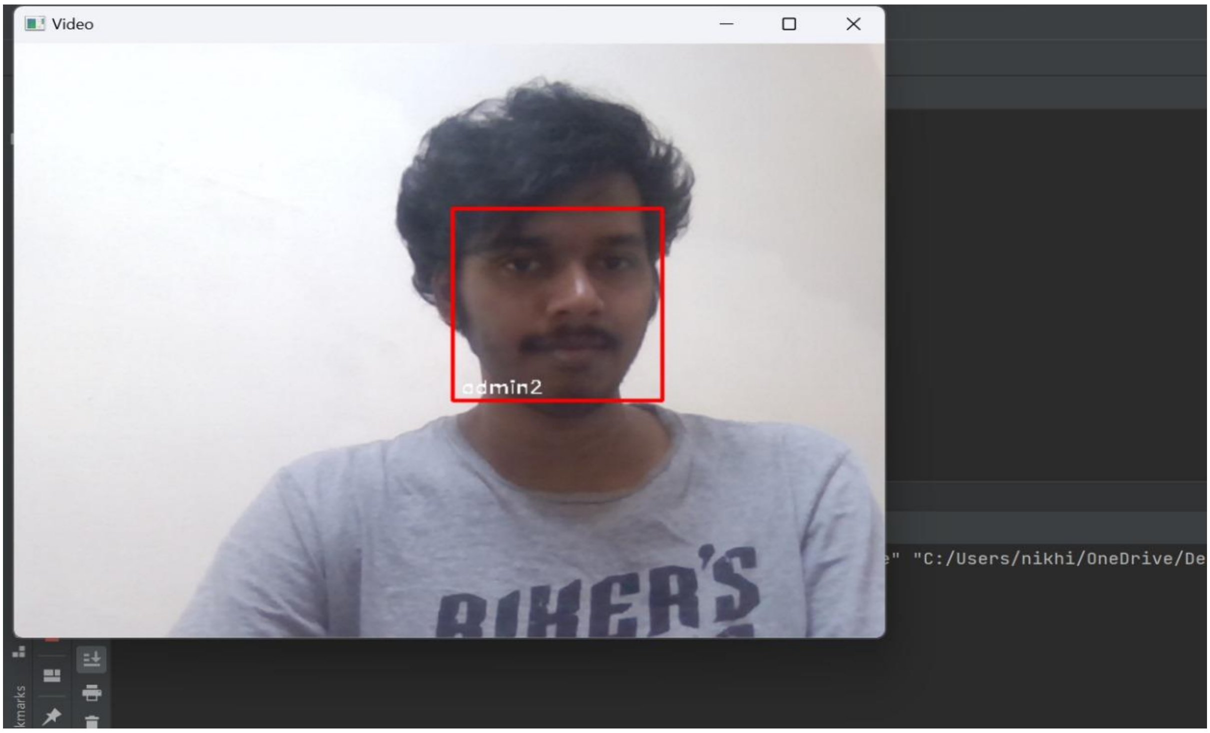


Fig 3: Before Restricting the file access



```
e" "C:/Users/nikhi/OneDrive/De
```

Fig 4: Face Recognition of one of the admin

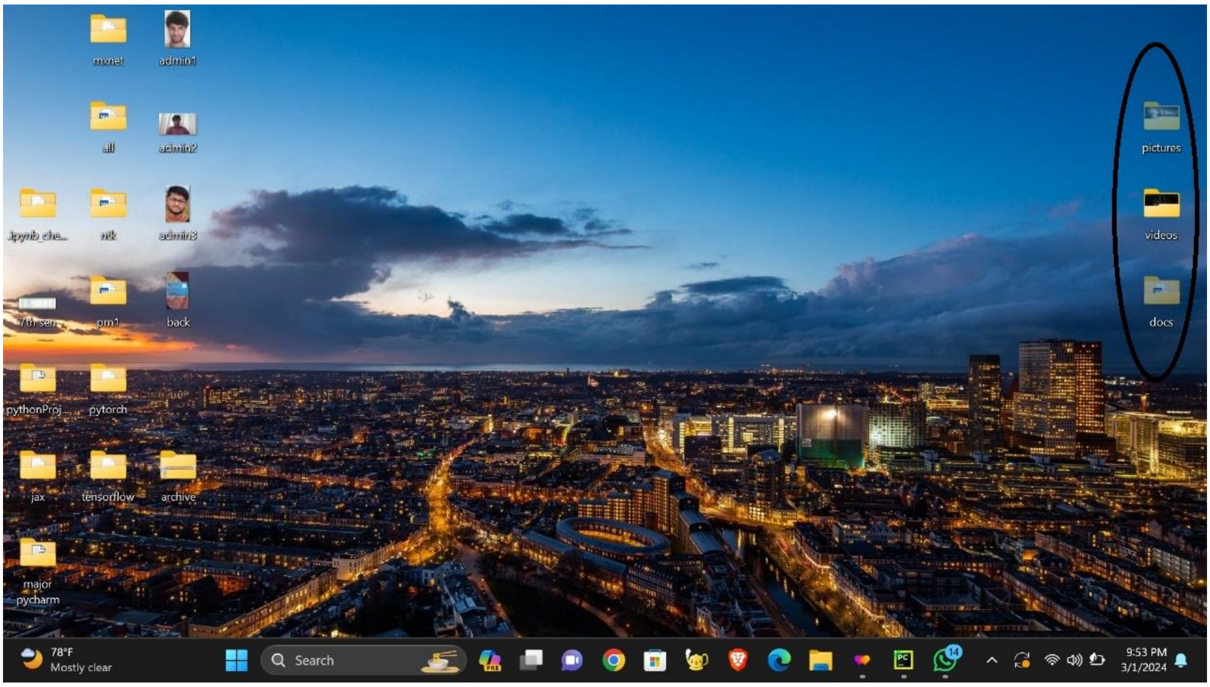


Fig 5: File access restriction based on face recognition

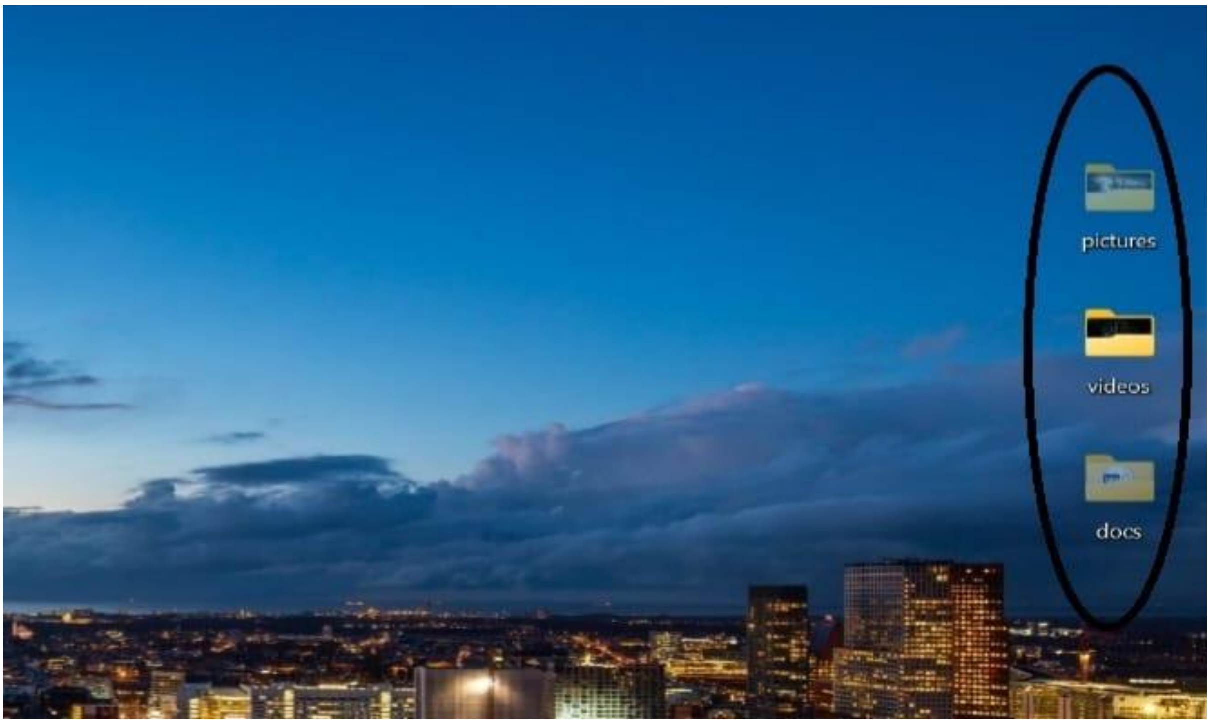


Fig 6: Final Outpu

CHAPTER-6

6. Conclusion and Future Enhancement

In Conclusion, this project successfully demonstrates the capabilities of Long Facial recognition systems as compared to normal file access control methods. It implements a framework for accessing the files based on the features extracted from a set of existing image files. The project achieves the following:

1. **Data Preprocessing**: Successfully extracts images from provided files and compares them to the image.
2. **Feature Extraction**: Extracts relevant features from the image, providing essential information for the model.
3. **Facial detection:** Detects the faces in the database, if the features match, the file will be opened and if not asks for a relevant question.
4. **Access control**: Access control only enables the files to be opened for the right user.
5. **Intruder Detection**: Uses the trained model to detect intruders, sending the concerned parties an image of them via mail.

However, there areas to consider:

Spoofing: Facial detection may be vulnerable to spoofing attacks, where an unauthorized person can use a photo, video, mask, or other means to impersonate an authorized person and gain access. This may require additional anti-spoofing measures, such as 3D face check or liveness detection.

Operating systems: Facial detection may not be compatible with all operating systems or platforms, or may require specific hardware or software to function properly. This may limit the availability and scalability of facial detection access control systems.

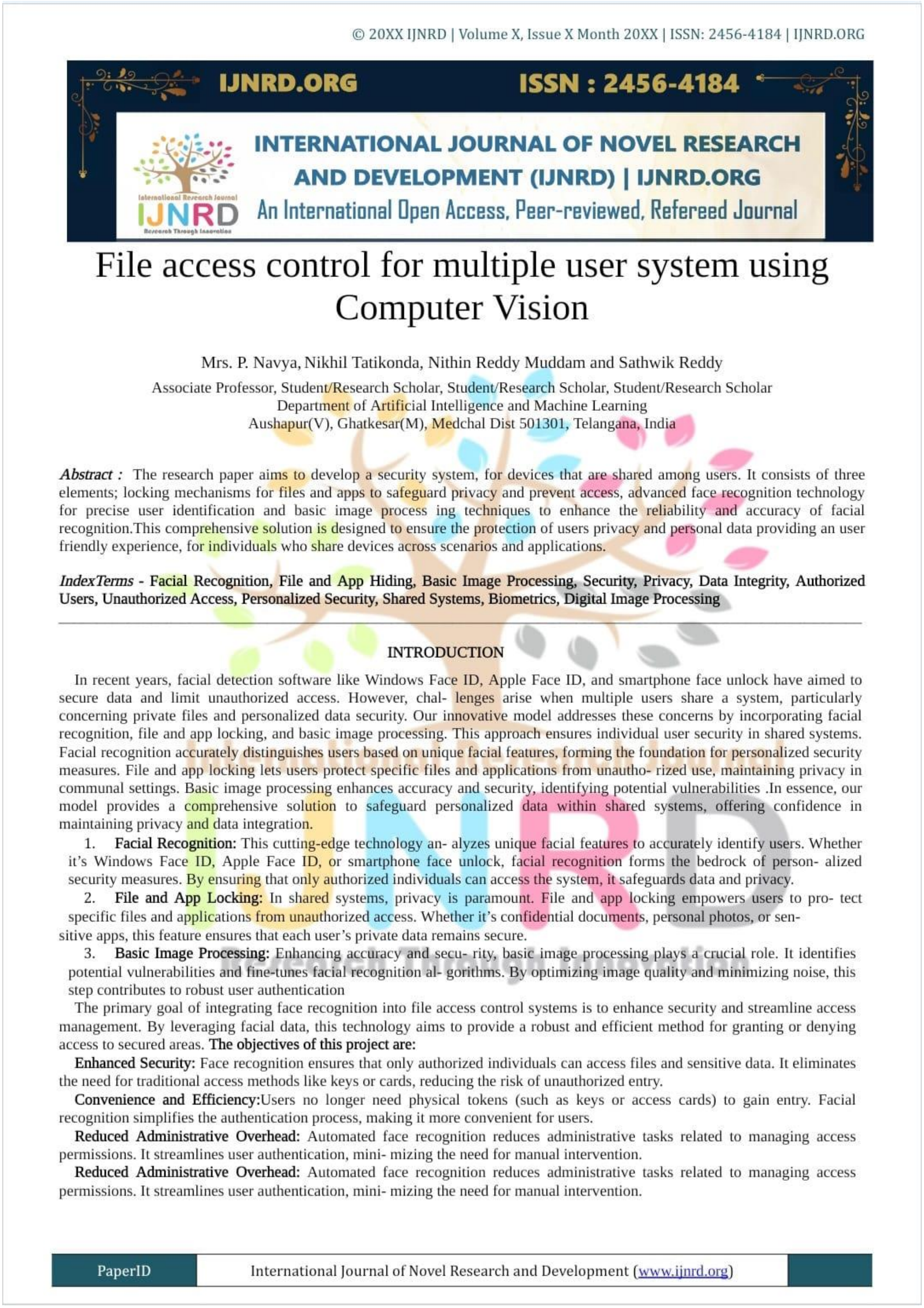
Privacy: Facial detection may raise privacy concerns, as it involves collecting, storing, and processing biometric data of users. This may require compliance with data protection laws and regulations, such as GDPR or CCPA, and consent from users. This may also pose risks of data breaches or misuse by hackers or third parties

here are **some further enhancements** to consider for this music generation project:

- **Using AI to improve accuracy and anti-spoofing:** AI-driven identity verification for access control can become more capable and accessible in the future. AI can enable facial recognition systems to incorporate multifactor authentication, video authorization, and other features to create a more secure and convenient access control solution.
- **Integrating with other biometric modalities**: Facial recognition can be combined with other biometric modalities, such as iris, fingerprint, or voice, to provide a more robust and reliable access control system. This can also increase the user acceptance and trust in the technology.
- **Adapting to different environments and scenarios**: Facial recognition can be enhanced to work in different lighting, angles, expressions, or occlusions, and to support and enforce mask-wearing mandates. This can improve the performance and usability of the technology in various settings and situations.
- **Implementing real-time facial recognition with Node.js and OpenAI:** Facial recognition can be implemented using Node.js and OpenAI, which are high-performance backend technologies and advanced artificial intelligence platforms. This can enable real-time facial recognition for access control with low latency and high scalability.
- **Ensuring privacy and compliance**: Facial recognition can be improved to ensure the privacy and compliance of the users and the data. This can involve using encryption, anonymization, consent, and audit mechanisms to protect the biometric data from breaches or misuse. This can also involve following the data protection laws and regulations, such as GDPR or CCPA.

CHAPTER-7

7.Published Paper



IJNRD.ORG ISSN : 2456-4184

International Research Journal
IJNRD
Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

File access control for multiple user system using Computer Vision

Mrs. P. Navya, Nikhil Tatikonda, Nithin Reddy Muddam and Sathwik Reddy

Associate Professor, Student/Research Scholar, Student/Research Scholar, Student/Research Scholar
Department of Artificial Intelligence and Machine Learning
Aushapur(V), Ghatkesar(M), Medchal Dist 501301, Telangana, India

Abstract : The research paper aims to develop a security system, for devices that are shared among users. It consists of three elements; locking mechanisms for files and apps to safeguard privacy and prevent access, advanced face recognition technology for precise user identification and basic image process ing techniques to enhance the reliability and accuracy of facial recognition.This comprehensive solution is designed to ensure the protection of users privacy and personal data providing an user friendly experience, for individuals who share devices across scenarios and applications.

***IndexTerms* - Facial Recognition, File and App Hiding, Basic Image Processing, Security, Privacy, Data Integrity, Authorized Users, Unauthorized Access, Personalized Security, Shared Systems, Biometrics, Digital Image Processing**

INTRODUCTION

In recent years, facial detection software like Windows Face ID, Apple Face ID, and smartphone face unlock have aimed to secure data and limit unauthorized access. However, chal- lenges arise when multiple users share a system, particularly concerning private files and personalized data security. Our innovative model addresses these concerns by incorporating facial recognition, file and app locking, and basic image processing. This approach ensures individual user security in shared systems. Facial recognition accurately distinguishes users based on unique facial features, forming the foundation for personalized security measures. File and app locking lets users protect specific files and applications from unautho- rized use, maintaining privacy in communal settings. Basic image processing enhances accuracy and security, identifying potential vulnerabilities .In essence, our model provides a comprehensive solution to safeguard personalized data within shared systems, offering confidence in maintaining privacy and data integration.

1. **Facial Recognition:** This cutting-edge technology an- alyzes unique facial features to accurately identify users. Whether it's Windows Face ID, Apple Face ID, or smartphone face unlock, facial recognition forms the bedrock of person- alized security measures. By ensuring that only authorized individuals can access the system, it safeguards data and privacy.
2. **File and App Locking:** In shared systems, privacy is paramount. File and app locking empowers users to pro- tect specific files and applications from unauthorized access. Whether it's confidential documents, personal photos, or sensitive apps, this feature ensures that each user's private data remains secure.
3. **Basic Image Processing:** Enhancing accuracy and secu- rity, basic image processing plays a crucial role. It identifies potential vulnerabilities and fine-tunes facial recognition al- gorithms. By optimizing image quality and minimizing noise, this step contributes to robust user authentication

The primary goal of integrating face recognition into file access control systems is to enhance security and streamline access management. By leveraging facial data, this technology aims to provide a robust and efficient method for granting or denying access to secured areas. **The objectives of this project are:**

Enhanced Security: Face recognition ensures that only authorized individuals can access files and sensitive data. It eliminates the need for traditional access methods like keys or cards, reducing the risk of unauthorized entry.

Convenience and Efficiency: Users no longer need physical tokens (such as keys or access cards) to gain entry. Facial recognition simplifies the authentication process, making it more convenient for users.

Reduced Administrative Overhead: Automated face recognition reduces administrative tasks related to managing access permissions. It streamlines user authentication, mini- mizing the need for manual intervention.

Reduced Administrative Overhead: Automated face recognition reduces administrative tasks related to managing access permissions. It streamlines user authentication, mini- mizing the need for manual intervention.

Figure 1. System Architecture

The above chart displays the architecture of the model. We can get an understanding of the design of the proposed model.

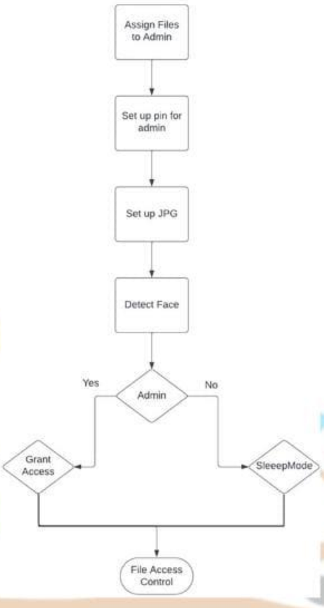


Figure 2. Flow chart of proces

EXPERIMENTAL RESULTS

The below are the images of the result after running our code.

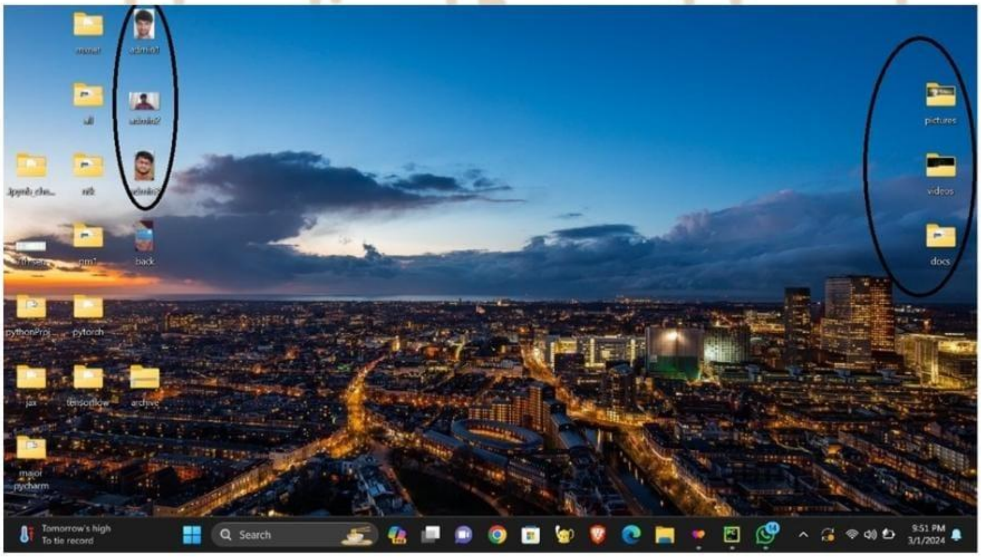


Figure 3. Before restricting the file access

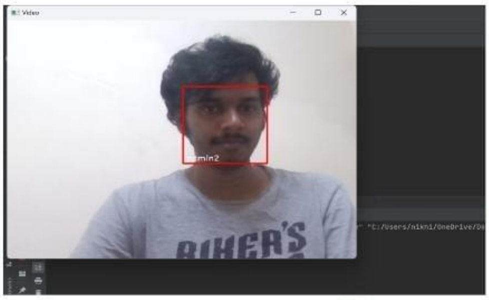


Figure 4. Face recognition of one of the admins

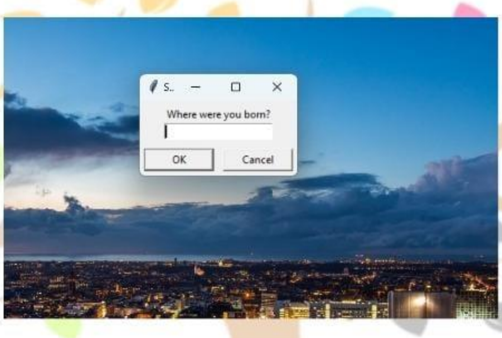

Where were you born?

Figure 5. security question for second step verification

Figure 6. Hiding the files

CONCLUSION

In Conclusion, this project successfully demonstrates the capabilities of long facial recognition systems as compared to normal file access control methods. It implements a framework for accessing the files based on the features extracted from a set of existing image files. The project achieves the following:

1) **Data Preprocessing:**Successfully extracts images from provided files and compares them to the image.
2) **Feature Extraction:** Extracts relevant features from the image, providing essential information for the model.

4) **Access control:** Access control only enables the files to be opened for the right user.
5) **Intruder Detection:** Uses the trained model to detect intruders, sending the concerned parties an image of them via mail.

One of the main limitations to consider is

1. **Operating systems:** Facial detection may not be com- patible with all operating systems or platforms, or may require specific hardware or software to function properly. This may limit the availability and scalability of facial detection access control systems. The below are some possible advancements in AI in future.

2. **Using AI to improve accuracy and anti-spoofing:** AI- driven identity verification for access control can become more capable and accessible in the future. AI can enable facial recognition systems to incorporate multifactor authentication, video authorization, and other features to create a more secure and convenient access control solution.

3. **Integrating with other biometric modalities:** Facial recognition can be combined with other biometric modalities, such as iris, fingerprint, or voice, to provide a more robust and reliable access control system. This can also increase the user acceptance and trust in the technology.

4. **Adapting to different environments and scenarios:** Facial recognition can be enhanced to work in different lighting, angles, expressions, or occlusions, and to support and enforce mask-wearing mandates. This can improve the performance and usability of the technology in various settings and situations.

5. **Implementing real-time facial recognition with Node.js and OpenAI:** Facial recognition can be implemented using Node.js and OpenAI, which are high-performance back- end technologies and advanced artificial intelligence platforms. This can enable real-time facial recognition for access control with low latency and high scalability.

6. **Ensuring privacy and compliance:** Facial recognition can be improved to ensure the privacy and compliance of the users and the data. This can involve using encryption, anonymization, consent, and audit mechanisms to protect the biometric data from breaches or misuse. This can also in- volve following the data protection laws and regulations, such as GDPR or CCPA. The file access control using computer vision solves the security issue of secret files in a single user system where there can be multiple admins. And also makes the pc not accessible to unknown users by forcing the sleep mode. It utilizes computer vision, face recognition and os to make all these possible

Acknowledgment

We would like to thank Mrs. P. Navya for her valuable comments and suggestions to improve the quality of the paper. We are also grateful to Dr. K. Shirisha Reddy for helping us review our work regularly. We would also like to thank the Department of Computer Science Engineering (AI and ML), VBIT Hyderabad for providing us with all the help we needed.

References

[1]Rana Hamid, “Develop of security system using facial recognition,” https://www.researchgate.net/publication/341261991_Home_ Automation_Security_System_Based_on_Face_Detection_and_ Recognition_Using_IoT.

[2] Arun Balasubramanyam, Mary E. Rudden and Donald E. Schaefer et al, “Access controller that controls access to files by using access control list,” https://shorturl.at/vzDJ0.

[3] Takahisa Shirakawa et al, “File access destination control device and method,” https://shorturl.at/rxBW4.

[4] Ashi Tyagi and Rahul veer Singh et al, “Data hiding techniques using steganography algorithms,” https://www.researchgate.net/publication/ 342261832_Data_Hiding_Techniques_Using_Steganography_ Algorithms.

[5] Micheal, Amer, Gerges and Nidal, “Face recognition security sys tem,” https://www.academia.edu/11766244/Development_of_Security_ System_using_Facial_Recognition. [

6] Hoo-Ki Lee, Sung-Hwa Han and Daesung Lee et al, “Kernel-based container file access control architecture to protect important application information,” https://shorturl.at/lmBHQ.

[7] Akihiro Urano, Takaki Nakamura, Hitoshi Kamei, Masakuni Agetsuma and Yasuo Yamasaki et al, “Face recognition security system,” https: //shorturl.at/bcx25.

[8] Rossana Ducato et al, “Data protection, scientific research, and the role of information,” https://www.sciencedirect.com/science/article/pii/ S0267364920300170.

[9] Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer, Josef Küng et al, “A systematic literature review for authorization and access control: definitions, strategies and models,” https://rb.gy/q1y94t.

[10] Sana Ghafoor, Dr Khattak, “Home automation security system based on face detection and recognition using iot,” https://www.researchgate.net/ publication/259027363_Face_Recognition_Security_System

CHAPTER-8

8. References

1. Data Hiding Techniques Using Steganography Algorithms by Rahul Veer Singh et al:

   https://www.researchgate.net/publication/342261832_Data_Hiding_Techniques_Using_Steganography_Algorithms

2. File access destination control device and method by Takahisa Shirakawa et al: https://www.researchgate.net/publication/302650915_File_access_destination_control_device_and_method?_sg=EER5znuiiuARFvasG3rZYWLsckxwEodOPx3W1qdvrwPyXjGJRpS_OPcrZpcUsddRwr2OqDqpQcriQKY&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

3. Control of access to files by Arun Balasubramanyam, Mary E. Rudden and Donald E. Schaefer et al : https://www.researchgate.net/publication/302805950_Control_of_access_to_files?_sg=0HR4g8pR04RX29MIcuoGKgOjGwT5hmsi0D3vET62Cjd6on_YDRm1dxbR50zTVnZG7yOUh8LJChw6iD0&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

4. Access controller that controls access to files by using access control list by Akihiro Urano, Takaki Nakamura, Hitoshi Kamei, Masakuni Agetsuma and Yasuo Yamasaki et al :

https://www.researchgate.net/publication/302670424_Access_controller_that_controls_access_to_files_by_using_access_control_list?_sg=ewxkt-NHAZ8eHn8sU2bOtqctRTDIvWnue5ydb6w_nBq7D0s7tfenpLl8qwgRFOEKunoirntiP1nA9rA&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

5. File access destination control device and method by Takahisa Shirakawa et al : https://www.researchgate.net/publication/302650915_File_access_destination_control_device_and_method?_sg=EER5znuiiuARFvasG3rZYWLsckxwEodOPx3W1qdvrwPyXjGJRpS_OPcrZpcUsddRwr2OqDqpQcriQKY&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ

6. Data protection, scientific research, and the role of information by Rossana Ducato et al : https://www.sciencedirect.com/science/article/pii/S0267364920300170

7. A systematic literature review for authorization and access control: definitions, strategies and models by Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer, Josef Küng et al : https://www.emerald.com/insight/content/doi/10.1108/IJWIS-04-2022-0077/full/pdf?title=a-systematic-literature-review-for-authorization-and-access-control-definitions-strategies-and-models

8. Data Hiding Techniques Using Steganography Algorithms by Ashi Tyagi and Rahul veer Singh et al : https://www.researchgate.net/publication/342261832_Data_Hiding_Techniques_Using_Steganography_Algorithms

9. Home Automation Security System Based on Face Detection and Recognition Using IOT by Sana Ghafoor, Dr Khattak : https://www.researchgate.net/publication/259027363_Face_Recognition_Security_System

10. Develop of Security System Using Facial Recognition by Rana Hamid : https://www.researchgate.net/publication/341261991_Home_Automation_Security_System_Based_on_Face_Detection_and_Recognition_Using_IoT