DIGITAL IDENTITY VERIFICATION THROUGH WEB BASED FACIAL RECOGNITION

G. Manisha[1], Reddyvari Venkateswara Reddy[2], Nemali James Suvishal[3], Bijja ManiKanth[4], Duddeda Bhanu Prasad[5]

[1, 2, 3] Student, Department of CSE (Cyber Security), CMR college of engineering & technology, Hyderabad, Telangana, India

[4] Associate Professor, Department of CSE (Cyber Security), CMR college of engineering & technology, Hyderabad, Telangana, India

[5]Associate Professor, Department of CSE (Cyber Security), CMR college of engineering & technology, Hyderabad, Telangana, India

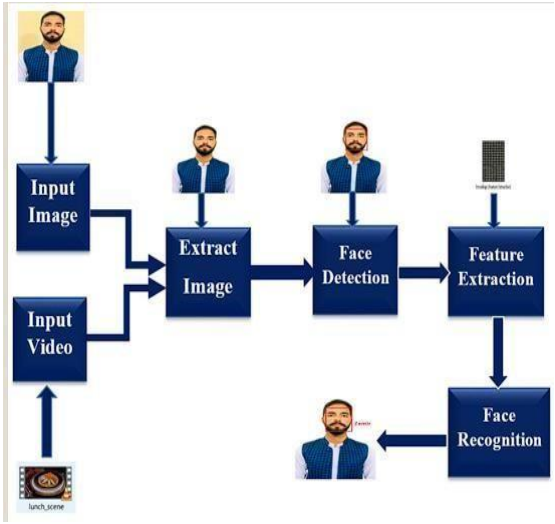
ABSTRACT: Live biometric systems should be used since the reliance on inadequate security procedures and approaches an ever-increasing number of assaults on authentication systems. That are recognized source of reliable authentication. Systems for password- based authentication are widely used and have many advantages. They must, however, be committed to memory vulnerable to dictionary, password guessing, and password resetting assaults from malicious parties. An alternative are biometric-based authentication methods, which don't require user memorization and difficult to replicate since they require the end users' physical presence. However, because there are more attacks every day, an attacker can trick the system by making a false or previously. Usinga web interface to analyze a user's facial traits, web-based facial authentication provides a safe way to confirm that person's identification. By utilizing the camera on a device, it takes pictures of faces, examines distinctive features, and then compares it with previously saved information to authorize access or verify a user. Convenience and security are combined with this technology to provide a seamless online service access experience that prioritizesuser privacy and data protection.

Keywords—identification, protection, authentication, vulnerable, technology

INTRODUCTION

The current technology used by hackers may crack any standard password and easily obtain access to highly sensitive resources, putting any company/organization, or even an entire country, at risk. At that point, more advanced security plans and techniques become important. The existing methods rely on using the person's biometric characteristics to carry out the identification process. Although these systems have a better identification rate, they are nevertheless susceptible to cyberattacks, such as the photo attack, which is among more common attacks of biometric recognition. Liveness detection is required toensure that the individual being tested for authentication is the actual user, ensuring that highly valued system resourcesare preserved and. Facial recognition will be assessed fromseveral highly important aspects such as Facial recognition in mobile application, Real time face recognition. Faceauthentication is often exposed to two kinds of break throughs, which are the image-based fraud and video-basedfraud attacks when the hacker exploits the front image ora video of the victim's face. Proposed a system that checks theuser.

comprehensive database of authorized users will be created, storing their facial features and access permissions. The systems performance will be evaluated using diverse datasets and real-world scenarios, measuring key metrics such as detection rate, recognition speed, and false positive/negative rates. By successfully implementing this application, a that user recognition and access provision system using face detection will be developed.



1. LITERATURE REVIEW

- Nawaf Hazim, Sinan Sameer Mahmood, Wael Esam Matti, "Face Recognition: A Literature Review", International Journal of Applied Information Systems (IJAIS), Volume 11 – No. 4, (September 2016): This research paper explains different techniques of face authentication and information gathering.

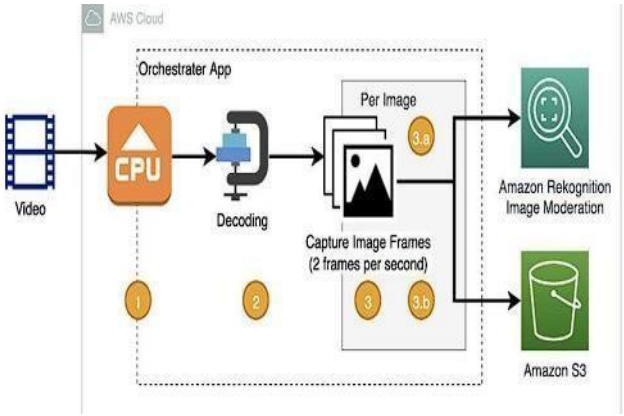
- W. Zhao, R. Chellappa, P.J.Phillips, A.Rosenfeld, "Face Recognition: A Literature Survey", ACM Computing Surveys, Vol. 35, No. 4, (December 2003): Explain about digital face authentication process and how each

information is work

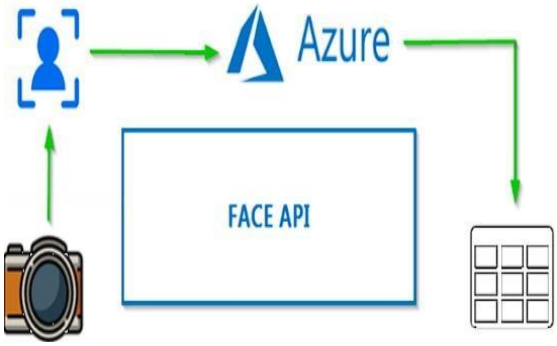
- M.Tamilselvi1,Dr.S.Karthikeyan,"ALiterature Survey in Face Recognition Techniques", No. 16, (2018): Explain about web based facial authentication and the different types of information gathering techniques. It briefly explains the working of facial authentication

2. EXISTING SOLUTIONS

Amazon Web Services offers a cloud-based image and video analysis solution called Amazon Rekognition. Because of its face detection and recognition features, that authenticate users and issue by recognizing and validating their faces.
Drawbacks:
Privacy Concerns: Amazon Rekognition has faced criticism and concerns regarding user privacy. Cost Considerations: The usage of Amazon Rekognition comes with associated costs



Microsoft Azure Face API: Azure Face API is a cloud- based service offered by Microsoft Azure. Provides face detection, recognition, and identification features. Developers can utilize to build applications for user recognition and access control scenarios.
Drawbacks:
Performance and Latency: The performance and report time of Microsoft Azure Face API can vary



Luxand Face SDK: Luxand developers to integrate face detections.
Drawbacks:
Platform Limitations: Luxand FaceSDK may have limitations in terms of platform compatibility. It may not support all operating systems or hardware configurations, which can restrict its usage in certain

3. PROPOSED SOLUTION

3.1 PROBLEM DEFINATION:

- Threats to cyber security are growing, which has prompted facial recognition systems that put security and privacy of data first.

- These technologies include features like remote session recording, user confirmation, and idle session timeout. Research has been performed to ensure secure devices, programs, and information for businesses.

- However, identity theft remains a risk, potentially compromising network infrastructure. Before permitting network, use or granting access to sensitive data, businesses must verify user identities to make sure security and privacy are upheld.

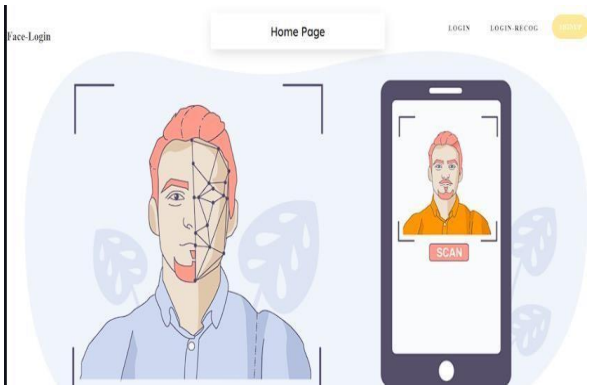
3.2 PROPOSED METHODS:

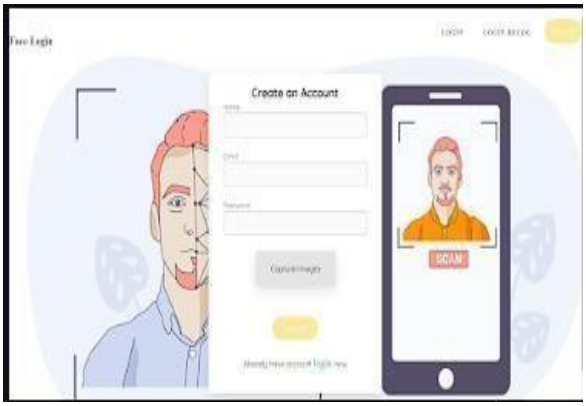
The proposed system for user recognition and access provision using face detection aims to create a robust and efficient solution for secure access control. The system will leverage face detection, recognition, and access provision components to achieve accurate user identification and authentication. During the user enrollment procedure, authorized can register their facial details in the system. Key facial traits will be extracted from the system.

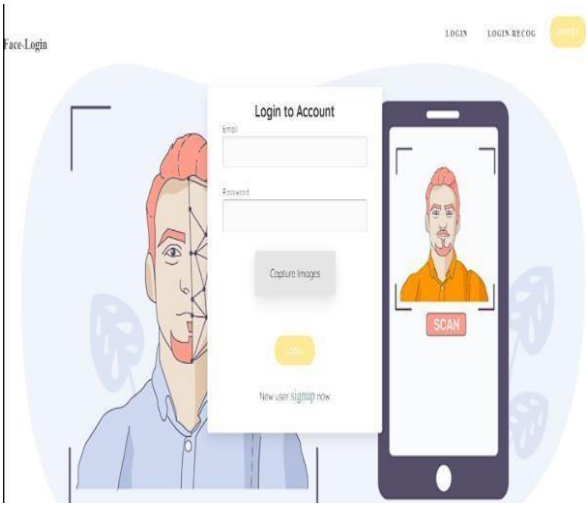
High-resolution photographs of the user's face upon enrollment. These user data and access rights, will be safely database. For real-time access control, the system will employ advanced face detection algorithms to detect and locate faces in images. To ensure accurate detection performance, these algorithms will be tuned to manage differences in lighting conditions, stances, and occlusions. The system will extract important facial traits, including landmarks, contours, and texture information, after faces have been recognized. These characteristics will function as distinct IDs for every person and be compressed into a small representation for effective comparison and storage.

After that, the system will compare the extracted facial traits with end user identity that have been saved in data using face recognition algorithms. The face recognition component will measure similarity scores and apply decision thresholds to identify the user's identity. In the task that the similarity score surpasses the predetermined threshold, the profile will be deemed authenticated and permitted access, according to their access rights, to the requested resources, locations, or services. The frontier of the system will be easy to use, making it easier to provision access, enroll users, and monitor. The capacity to control user profiles, access rights, and track system performance will be granted to administrators. We shall keep audit trails and logs. Its will be outline for simple unification with old infrastructure, such as access control systems, databases, or network protocols. It will be developed to be scalable, accommodating a growing number of users and supporting concurrent access requests, the proposed system aims to deliver accurate and efficient user recognition and access provision using face detection

- Sign up with details
- Open login page
- Capture the image
- Press the enter button







3.3 METHODOLOGY:

- Registration with valid username and password along with the photo of the user.
- The web cam the picture is captured and is stored in the database which is mongo db.
- Mongo Db is meant for storing user's credentials and is very efficient in handling data. It also provides additional security.
- Picture of the user matches with the image that is stored in the database then the access will be provided to the end user.

3.4 IMPLEMENTATION:

Face identification applications use AI algorithms, ML, mathematical analysis and image processing to find faces within images and distinguish them from nonface objects like landscapes and other facial parts. Before face detection begins, the analyzed media is preprocessed to improve its quality and remove images that might interfere with identify.

Facial identification algorithm start by scanning for man eyes, among the simple feature to detect. They then try to detect facial

landmarks, such as eyebrows and irises. The algorithm does extra tests to verify that it has identified a face after determining that it has located a facial region.

Huge data sets boasting thousands of positive and negative photos are used to train the algorithms in sequence to guarantee accuracy. The algorithms are better at identifying faces in an image and where they are thanks to the training.

controller: This is like the brain of the operation, where all the main instructions are.

docs: Here we keep all the documents that explain how everything works.

Face auth: This folder is dedicated to the actual facial recognition part.

logs: Any records of what the system does go here, so we can look back if we need to.

static: This is for files that don't change often, like images or styles for the website
.
templates: These are the blueprints for how web pages will look

business val: This is where we make sure that what we're building is valuable for the business.

Data access: This is all about how we get to and manage the data we need.

entity: we define the types of data we're dealing with.

configuration: This is where we set up the settings for how the system should work.

3.5 DESCRIPTION:

The objective of a Web Based Facial Authentication using an Face net and uses flask server for running keras neural network model and MongoDB as database

3.6 ADVANTAGES OF PROPOSED SYSTEM:

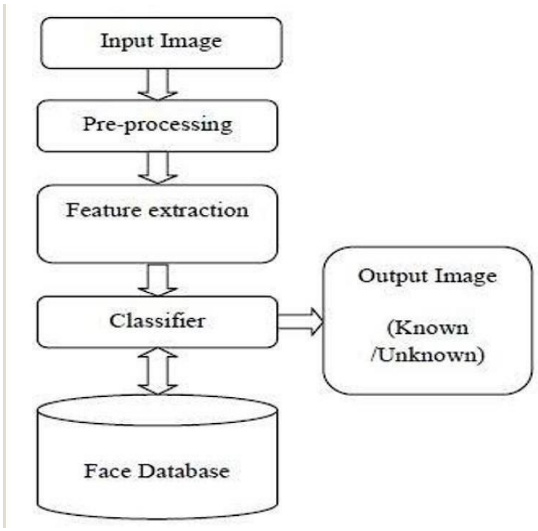
- It provides the strong security for protecting the data
- It has unique and secure authentication methods
- It maintains privacy of the user
- It prevents from the frauds

3.1 SYSTEM REQUIREMENTS:

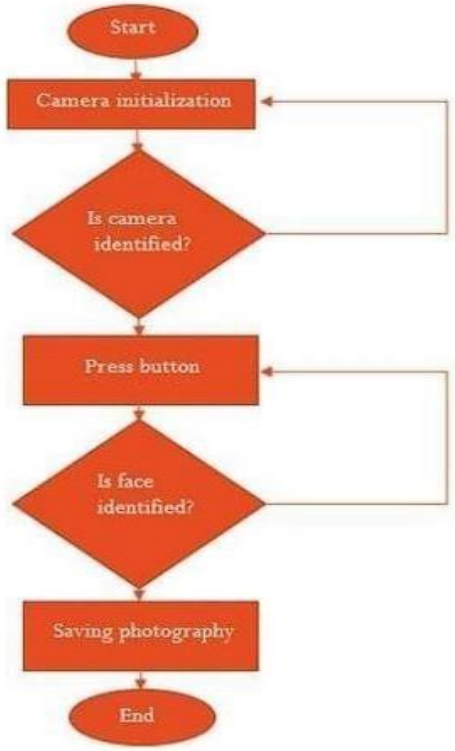
Hardware System Configuration:
Hard disk: 200GB
Monitor: Standard LED monitor System: I3 processor
RAM: 4GB

Software System Configuration:
Operating System: Windows 8/10 Coding Language: Python, HTML, CSS. Database: Mongo DB

3.2 BLOCK DIAGRAM:



3.3 FLOW CHART:



4. LIMITATION:

Many different adaptations, tests to continue work on this framework until the implementation phase. Concerning the results of the above applications we can also expect to improve them by having richer authentication, with more attributes and less limitations. Furthermore, particular mechanisms like continuous authentication based on face recognition. Consequently, proposing secure application having liveliness and continuous authentication for the user with stronger algorithms. There is also a plan for developing a system that combines both liveness detection and continuous authentication features. Moreover, the system will be tested in different conditions to solve challenges faced inentity time face recognition.

- The Effectiveness of Facial Recognition Is Limited by Poor Image Quality The effectiveness of facial recognition algorithms is influenced by image quality. When compared to a digital camera, the image quality obtained from scanning video is relatively poor. Even high-definition video is typically 720p, with a maximum resolution of 1080p (progressive scan). These numbers translate to roughly 2MP and 0.9MP, respectively, but a low-cost digital camera can capture 15MP.

- Small Facial identification becomes complicated with Smaller Image Sizes A face-detection algorithm's ability to identify a face in picture or a still from a videocapture depends on how big the face is in relation to themeasurement of the whole image. The recognized face is just 100 to 200 pixels on a side due to the already modest image size and the target's distance from the camera. In addition, the duty of scanning an image for different face sizes requires a much processing power. The majority of algorithms include face-size range specification in demand to reduce false positives duringdetection and expedite image processing.

5. RESULT:

Now the world becomes more and more better the advance in science and technology, so face recognition is slowly recognized by people, and we also began to use it indifferent fields. Face recognition is the use of human facialfeatures to complete identification.

The research also identified the challenges faced in user recognition, including the difficulty in ensuring the security and integrity of biometric data transmitted over remote connections. The findings highlight the importance of using robust encryption and secure communication channels to protect sensitive user information during the authentication process.

6. CONCLUSION:

Various biometric recognition and authentication, but none meet the necessary criteria for effective verification and continuous authentication.

These include high detection rate, continuous authentication, low cost, minimum complexity, and high security.

A security solution is needed that pushes all these criteria for continuous, effective authentication and verification, contributing to current security standards wherever it is deployed.

7. REFERENCES

1. Secure and structured acs for remoteauthentication using one time password andbiometrics" by Gaurav Gupta and AmitChaudhary(2020) https://ieeexplore.ieee.org/abstract/document/8537829

2. “Remote Access Security Best Practices" by CiscoSystems” https://www.cisco.com/c/en/us/support/docs/security-vpn/anyconnect-secure-mobility client/116075-technote-anyconnect-00.html

3. “Security Considerations for Remote Access andBYOD" by Symanteccorporation” https://www.symantec.com/connect/articles/security-considerations

4. “Remote user authentication techniques" by SuryaPrakash, Harsh Kumar Verma, andNeelam Duhan(2021) https://www.sciencedirect.com/science/article/pii/S2352550917304432

5. "Secure Remote Access: Security BestPractices" by Microsoft https://docs.microsoft.com/en-us/windows-server/remote/remote-access/