Two-Layer Authentication for Secure Applications Using AI-ML

Rakshitha P [1], Rakshitha V [1], Ravuru Indu [1], Sushmitha H [1], Mrs.Keerthi Mohan[2]
[1] *Student, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bengaluru, India*
[2] *Professor, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bengaluru, India*

***Abstract*–Improved security is provided by two-layer authentication. A higher level of authentication assurance is provided by two-layer authentication, which is crucial for the security of online banking, voting systems, secure transactions, secure virtual meetings, etc. The two-layer authentication requirements for many banking systems are met by delivering a One Time Password (OTP), processed by an SMS, to the user's linked device. With mobile phones becoming more and more capable tools, a two-layer OTP based authentication strategy for secure applications has been developed. This two-layer authentication involves face recognition in the first layer followed by OTP generation. In our proposed approach we authenticate verified users and allow their access to the system and deny access to unauthorised person through this two-layer authentication. Our proposed system achieves better characteristics than the other systems. This proposed approach can be used for many applications such as online banking system, voting system, secure transactions, secure virtual meetings, etc.**

Key Words: **OpenCV, Python, facial-recognition, OTP generation, CNN**

I. INTRODUCTION

Two layer authentication is a security process in which the user provides two forms of identification, one of which is a physical identifier or biometric identification, and another that is easily remembered, such as a security code or password. The authentication process is broadly classified into two types namely traditional and biometric approach. In traditional approach, the authentication is based on text, alpha-numeric, image or one-time password, whereas in biometric approach the authentication is based on fingerprint, iris recognition and face recognition. The Fig.1.1 depicate the classification of authentication and its types.

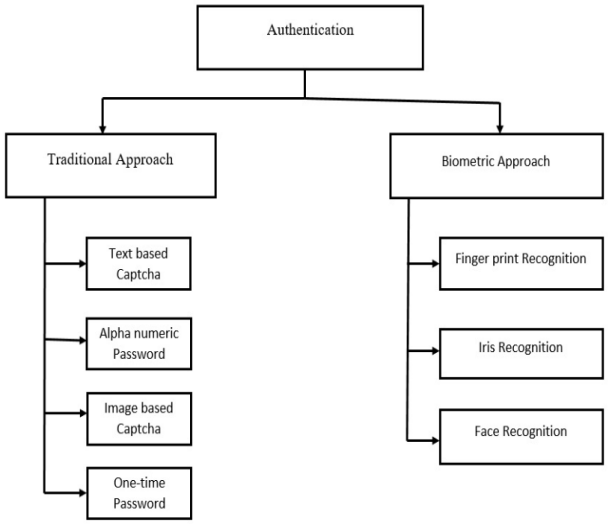

Fig.1.1: Classification of Authentication

In this proposed model, we combine both traditional and biometric process for authentication. The first level we use for authentication is facial recognition. Initially, that person's face is stored in the database when they first enter the system. Now, when a person wants to enter the system, their face matches a picture taken earlier that is stored in the database, and if the face matches, the person should be ready for the second layer of authentication. The second layer we use is based on OTP generation. Only if both authentications are successful, the person can access the system. The first layer must be completed before the second layer can be authenticated. This system can be used in places where a high level of security is required, such as banks, digital assessment environments, voting systems, security fields, Universities and government agencies.

One of the most popular identifying methods for online identity verification is biometric facial recognition. It is a technique for biometric

identification that makes use of measurements of the facial biometric patterns and data are used to confirm a person's identity using their head and face. To identify, verify, and authenticate each person, the system collects specific biometric information about their face and facial expressions for the verification purpose. One of the security requirements for common terminal authentication systems is to be simple, fast and secure, as people encounter authentication mechanisms every day and need to identify themselves using traditional data-based approaches such as passwords. However, these techniques are not secure because they can be seen by malicious observers who use monitoring methods such as shoulder surfing (an observer entering a password using a keyboard) to collect user credentials. Additionally, there are security issues caused by poor communication between systems and users. As a result, we propose a two-layered security framework to protect PIN codes, where users can enter a password via OTP.

The note of this paper is sort out as follows: In section II, we discuss about various proposed methods in our project. In section III, we discuss the implementation. In section IV, we discuss the results of our implemented project. Finally, the conclusion about two-layer authentications is covered.

II.PROPOSED METHOD

Proposed Technique:

- Passwords comes with a major security problems because they can be easily stolen by hackers using techniques such as snooping, shoulder surfing, guessing or sniffing.
- To avoid them, we proposed a model for two-layer authentication using facial recognition followed by OTP. If both factors are met, only then can a person enter the system.
- Two-layer authentication reduces the risk of data security breaches and keeps data secure.
- This system can be used in applications that require high security, such as online banking systems, voting systems, secure transactions, secure virtual meetings, etc.

III. IMPLEMENTATION

A. Image Acquisition

- Image acquisition is the process of capturing digital images from the real world using various imaging devices such as digital cameras, scanners, or sensors.
- The process involves converting analog data (light) into digital signals that can be stored and processed by a computer.

B. Pre-processing

Three procedures were completed during the pre-processing stage: face detection, face scaling, and face cropping using the Multi-Task Cascaded Convolutional Neural Network library(MTCNN). The position of the face in a given image was found using detection, and this location was then realised in the form of a bounding box. The cropping based on the bounding box was then put into practise. We first resize an image to various scales to create an image pyramid, which serves as the input of the following three-stage cascaded framework:

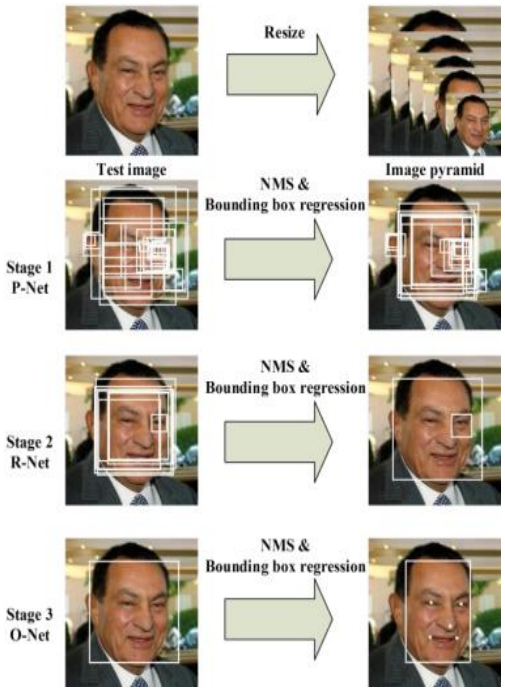

Fig. 3. 1 depicts the overall pipeline of our method.

Stage 1: Using the Proposal Network (P-Net), a fully convolutional network, we extract the candidate windows and their bounding box regression vectors in this stage. Following that, the candidates are calibrated utilising the determined bounding box regression

vectors. Then, candidates with a lot of overlap are combined using non-maximum suppression (NMS).

Stage 2: All candidates are submitted to Refine Network (R-Net), a different CNN that further rejects a substantial proportion of incorrect claims.
Stage 3: This stage is comparable to Stage 2, except that it focuses more on describing the face in depth. The network will specifically output the locations of five face landmarks.

C. Feature Extraction
Feature extraction is the process of extracting relevant information or features from an image that can be used to represent and analyze the image.
Feature extraction is typically performed after image preprocessing, which involves various techniques such as filtering, segmentation, and normalization, to enhance the quality of the image and make it more suitable for feature extraction.

FaceNet:
Google researchers created FaceNet by employing a Deep Convolutional Neural Network (DCNN) to translate photos of a person's face into Euclidean spaces (groups of Geometric points) that are also referred to as embedding. Embedding is determined by the degree of similarity and differences between faces, so that if the faces are similar, the value will be closer, and if they are different, the value will be distant.
Typically, when using the FaceNet model to extract features, as illustrated in Fig. 3.2, the input images will enter the deep learning architecture, be normalised L2, and then produce facial features (embedding) that are trained using Triplet Loss.

Fig. 3.2 Feature Extraction using FaceNet

D. Classification using CNN
Convolutional Neural Networks (CNN) is a deep learning algorithm that is particularly useful for image classification. In image classification, the objective is to assign a label or category to an input image.
A CNN consists of multiple layers of filters that extract increasingly complex features from the image. These layers include convolutional layers that apply filters to the image to extract features, and fully connected layers that classify the image based on the learned features.

E. OTP Generation
Bots are external application that operate inside Telegram. Bots can be communicated with by users through messages, commands, and inline requests. Using HTTPS queries to our Bot API, we can manage bots. The actions that must be taken are as follows:

- On Telegram, type in "BotFather."
- To begin, enter the command /start.
- To get a bot, type /newbot.
- Type your unique user name, which should end in "bot," and your bot name. You would then receive your Bot token.
- Once our token has been created, we'll write a Python script to build a Telegram bot that will transmit text, emojis, and stickers in response to user input.

IV.RESULTS

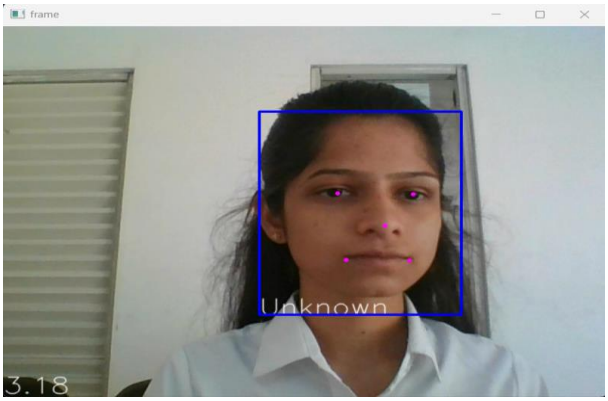

Figure 4.1: Displaying boundary, facial landmarks, face id, frequency

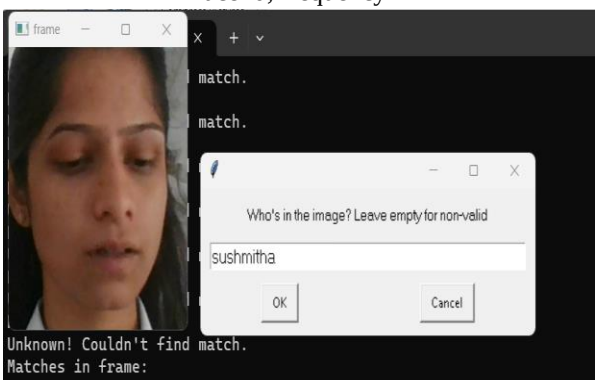

Figure 4.2: Pop-up window to save the unknown face

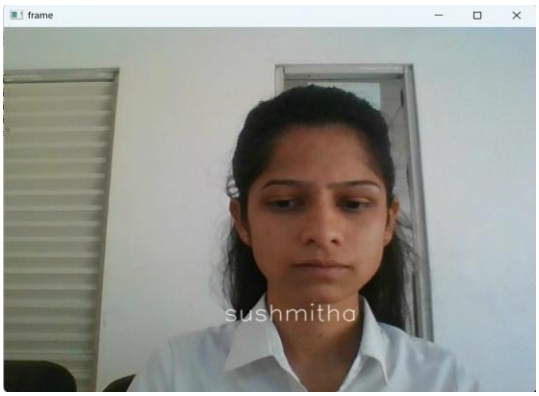

Figure 4.3: Saved face

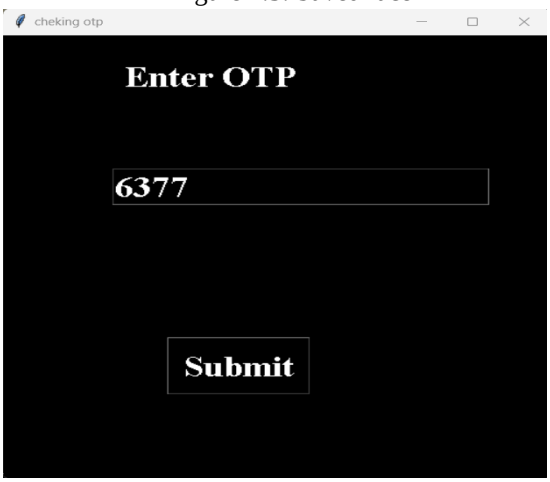

Figure 4.4: OTP submission

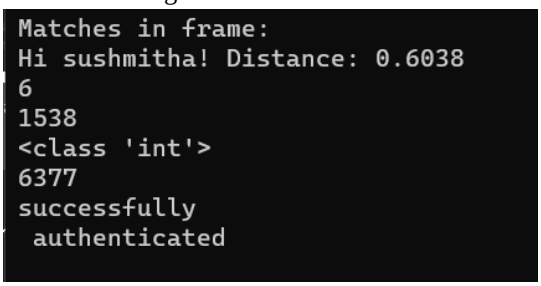

Figure 4.5: Authentication Successful

V.CONCLUSION

Passwords comes with a major security problem because they can be easily stolen by hackers using techniques such as snooping, shoulder surfing, guessing or sniffing. To avoid them, we proposed a model for two-layer authentication using facial recognition followed by OTP. If both factors are met, only then can a person enter the system. Two-layer authentication reduces the risk of data security breaches and keeps data secure. This system can be used in applications that require high security, such as online banking systems, voting systems, secure transactions, secure virtual meetings, etc.

REFERENCE

[1] Locker Security System using Facial Recognition and One Time Password(OTP) N. Anusha, A. Darshan Sai and B. Srikar: 2022

[2] Multi-Factor Authentication to Systems Login Bandar Omar ALSaleem and Abdullah I.Alshoshan:2021 IEEE

[3] Securing ATM using Face Recognition Authentication and OTP Parag Achaliya, Govind Bidgar, Hrutika Bhosale, Prasad Dhole and Kajal Gholap: March 2021

[4] Online voting system using face recognition and OTP(one time password) Dr. Sanjay Sange, Pranjali Gurao, Ishwari Pawar, Shruti Ragade and Akshada Zaware : International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume: 08 Issue: 06 June 2021

[5] Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token Muhammad Dandy Pramana, Anne Lestyea and Amiruddin:2020 IEEE

[6] Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control SystemBintang Wahyudono and Dion Ogi :2020 IEEE

[7] Face Recognition based new generation ATM system Dr S Sasipriya, Dr P. Mayil Vel Kumar and S. Shenbagadevi: European Journal of Molecular & Clinical Medicine, ISSN 2515-8260 Volume 7, Issue 4, 2020

[8] A Comparative Study on Facial Recognition Algorithms Sanmoy Paul and Sameer Acharya

[9] Smart Attendance System Using CNN Rajat Kumar Chauhan, Vivekanand Pandey and Lokanath M:International Journal of Pure and Applied Mathematics, Volume 119 , No.15 , 2018, ISSN:1314-3395

[10] E-voting Using One Time Password and Face Detection and Recognition Ayesha Shaikh, Bhavika Oswal, Divya Parekh and Prof. B. Y. Jani: International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February - 2014 I, JERT ISSN: 227