A Survey on 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]
Student, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bengaluru, India
Professor, Department of CSE, Dayananda Sagar Academy of Technology and Management, Bengaluru, India

***Abstract*–Two-layer authentication provides improved protection. Two-layer Authentication delivers a higher-level assurance of authentication, which is essential for online banking security, voting system, secure transactions, secure virtual meetings, etc. Many banking systems have satisfied the two-layer authentication requirements by sending a One Time Password (OTP), processed through an SMS to the user's connected device. A two-layer OTP based authentication scheme for secure applications has been proposed through SMS using mobile phones as they are becoming more and more powerful devices. 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.

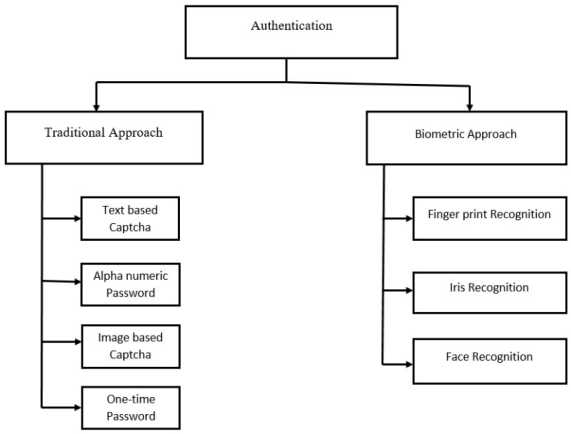

Fig.1.1: Classification of Authentication

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 various research carried out in two-layer authentication. In section III, we discuss the various parameters considered and their analysis. Finally, the conclusion about two-layer authentications is covered.

II.LITERATURE SURVEY

Anusha and et al, have proposed Locker Security System using Facial Recognition and One Time Password (OTP). This system was implemented to address current security issues in the cabinet system. In this system when a person needs to open the locker, he must enter the PIN code which is set by the user priory. If the entered PIN is correct, then the camera captures the image and compares with the user's image using Eigen-face method and PCA algorithm. The captured image is then verified with the images in the database with the Euclidean distance and Viola-Jones algorithm. If the images are matched, an OTP is generated to the registered user's mobile number as a text message via GSM service also an email notification is triggered. If the attributes didn't match, then the login information related to the event is sent to registered number and email id. The proposed system is more secure because user can open the locker only with password or OTP received. This system can be implemented for home security purpose at corridor and other places when embedded with motors and sensors.[1]

Bandar and et al, have proposed Multi-Factor Authentication to Systems Login which mainly deals with multi-factor authentication system. Multi-factor authentication combines convenient to use and cost effective. The system uses graphical passwords for authentication which deals with graphical pictures instead of text and numbers. Initially, at the recording stage, the user can select and save more than three pictures. At the sign in stage, the user must select only the valid pictures which was selected by the user during the recording phase, the pictures must be selected correctly with the same order as selected in recording phase. The system was proposed to decrease security threats such as screenshot attack, key hacking and shoulder surfing. This system also protects the user from installing malware or trojans, because this malware is a security issue which records user information and other details such as the user's screen, the user types on the keyboard. Malware can also access and change system files, and therefore the proposed system was designed to protect user information so that no program or malware can capture user's passwords, or the authentication methods used.[2]

Achaliya and et al, have proposed Securing ATM using Face Recognition Authentication and OTP. A traditional ATM system processes the ATM card and PIN or other secret key combination together to access the customer's account, increasing illegal activities such as card theft or PIN theft, card duplication and other criminal activities. The proposed system contains facial recognition technology, which is a computer application that naturally extracts or validates the contours of a person from a computerized image or video from a video source. The proposed system describes a facial recognition method for ATM system authentication. This system works in such a way that when a user inserts a card into an ATM to make transactions, the system asks for a PIN code, after which the user must enter a valid PIN code. After setting the PIN, the system will show two options: Face ID and OTP option. This system has been introduced to provide a suitable solution to a much smaller problem of ATM fraud using facial recognition which is possible only when the authorized account holder is present and in any emergency the account holder cannot come to the ATM and OTP facility is also available. Thus, it eliminates illegal transactions at ATMs without the

knowledge of the account holder. So using facial recognition method for authentication is to make ATMs more secure.[3]

Dr. Sanjay and et al, have proposed Online voting system using face recognition and OTP (one time password). In this paper, we proposed an online voting system for voting using facial recognition and OTP. The OTP and facial information are forwarded to the server unit for further verification. The server then checks the data in the database and compares the data already in the database. If the information matches the information already existing registration, the person can vote. If not, a message appears on the screen and the person is not allowed to vote. Voters elect voters. In the current situation, the voter has to present his voter card to vote in the booth. So this process is time consuming because the authorities have to verify the voter card. That is why we proposed a new system to speed up the voting process and avoid such problems.[4]

Dandy and et al, have proposed Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token. In this study, a secure access control system with dual facial recognition and SMS-Token OTP is proposed. Firstly, they have examined the study regarding the use of the ESP32 CAM in access control security and smart home. Secondly, two-step authentication access control system was designed based on facial recognition and TOTP-SMS-ID. Thirdly, an Arduino Uno platform is used to implement the proposed system using ESP32-CAM and SIM 800L as hardware and software components respectively. The web server on the ESP32-CAM board was used to perform functions on facial recognition. Initially, the user's face is scanned and detected using ESP32-CAM module. Once the scan is successful, the system validates the face of an individual and the system administrator sends an identification code generated by TOTP. This passcode is used in the authentication process. If the entered code is valid, then authentication is successful. If the code entered is invalid, the system rejects the procedure and returns the correct identification passcode.[5]

Bintang and et al, have made Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System. In this paper face recognition is implemented using LBP algorithm to overcome the vulnerability of face-false attacks. RFID is used in different fields like industrial automation, public transport, asset tracking, purchase and sale and many more used because it works well. Biometrics are very unique to each individual, therefore biometric such as facial recognition is used which provides more security compared to any other mechanisms. The implemented system stores the verified face token and compares it with the RFID token for users who's face is successfully authenticated. The proposed system involves two factor verification, if both the verification process is successful only then the authentication is obtained to register the presence of the user later notify the authenticated user with the message. Based upon the testing results and other analysis, the conclusions can be taken as follows:

• The ability of the pass-through system to detect fraud related to photo attacks is cent percent.

• The proposed system gives maximum accuracy using RFID and facial recognition.[6]

Dr. S Sasipriya and et al, have proposed Face Recognition based new generation ATM system. The proposed system is based on a facial recognition system which uses RFID tag to replace the use of ATM card. The facial image is used for verification purposes. Firstly, the captured user's image is verified with the image present in the database. An alert message is sent to the user when an unknown users face is detected in the system. The proposed system uses Raspberry Pi microcontroller in the control part. The implemented ATM transaction system provides high security through facial recognition and verification method. Thus, the system reduce forced transactions with improved security.[7]

Sanmoy and et al, have proposed A Comparative Study on Facial Recognition Algorithms. This paper describes different face detection algorithms and compares their detection accuracy. Faces are detected using the Haar Cascades algorithm, which is stored in the database, later to compare the exactness of the Eigen face detection with known algorithms PCA, KNN, SVM and CNN. The obtained conclusion claims that among the four algorithms used, CNN was concluded as the most effective one. The study's system architecture diagram describes how the camera will recognize human faces using the Haar Cascade algorithm. Considering the user's face recognition conditions, the recognized images are fed to the facial

classification algorithms, and then compares the accuracy among SVM, KNN and CNN algorithms.

Face classification module involves the following stages:

- Pre-processing: In this stage each image in the database is read and then converted to a dimensional matrix in accordance with its image. The images are normalized and finally split into train and test sets with a fraction of 0.2.
- PCA: The PCA algorithm is then implemented to both training and testing data images to bring out all the unique features from each image. Eigen values are then calculated from the PCA algorithm and 95% of the deviation is obtained.
- Classification module: The matrix obtained from PCA is then passed onto different facial recognition algorithms for training which is noted as classification process.
- Benchmark module: The comparisons are made among the recognition exactness of SVM, KNN, and CNN for the train as well as the test dataset, it was then found that CNN provided the more accuracy.

This study helps developers to select the best facial recognition algorithm among various existing algorithms that can be applied in retail stores, security systems and many other fields which require facial recognition techniques.[8]

Rajat Kumar and et al, have proposed Smart Attendance System Using CNN. This system is about a face recognition based on intelligent attendance system that can be used to track the attendance of students sitting in a classroom at the same time. The implemented system includes four parts. First, face detection is performed based on the histogram directional gradient (HOG) algorithm. Second, face alignment is performed based on the face orientation estimation algorithm. Third, an approach based on the Facenet algorithm is used to encode the face. Each face is coded with unique 128 values. Finally, an SVM classifier is trained with these 128 metrics for each face. This system also makes an attendance report with date, and it is automatically sent to the faculty. This system is non-intrusive and reduces the likelihood of proxies and false participation.[9]

An efficient manner Locker Security System Using Facial Recognition and One Time Password

Ayesha and et al, have proposed E-Voting system Using One Time Password and Face Detection and Recognition. In this paper, they have proposed an online voting system where election data can be stored and processed with a higher level of security. Firstly, facial recognition and identification system is used for authentication. In this authentication method, the persons face is captured by the web camera while voting. The second layer authentication is implemented using one time password. At the end of the first layer authentication, a random number is generated based on one time password which is used by the user while voting. These technologies provide high security that overcomes the vulnerability of the traditional voting system. The biggest advantage of electronic voting is that the user can vote more securely anywhere and anytime.[10]

The summary of type of authentication, number of parameters used for authentication and their applications are tabulated in Fig.1.2.

Reference	Two-factor	Multi-factor	Attributes	Applications
[1]	No	Yes	PIN, Face recognition, OTP	Home corridor security framework with sensors and actuators.
[2]	No	No	Graphical password	Authentication in computer system
[3]	Yes	No	PIN, Face recognition, OTP	ATM security
[4]	Yes	No	Face recognition, OTP	Online voting system
[5]	Yes	No	Face recognition, OTP	Access control system
[6]	Yes	No	RFID, Face recognition	Online voting system
[7]	Yes	No	RFID, Face recognition	ATM security
[8]	No	No	Face recognition	Retail stores, security system
[9]	No	No	Face recognition	Smart attendance system
[10]	Yes	No	Face recognition, OTP	E-voting system

Fig.1.2: Summary of Literature Survey

III.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 System Bintang 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