ISSN No:-2456-2165

Three Way Password Authentication System

[1]M UDAY KUMAR, [2]K VAMSI KRISHNA, [3]TS ABHIRAM, [4]NV RAVINDHAR
Department of Computer Science & EngineeringSaveetha Engineering College
Tamilnadu, India

Abstract:- Personal identification numbers (PINs) are frequently used to verify the identity of a user and for other security purposes. It is possible to crack the password via shoulder surfing or thermal monitoring while using PIN-based password authentication. Hands-free eye-blink PIN authentication. Instead, PIN input techniques leave no tangible evidence of the user's activity, making them a more secure alternative to entering a password. PIN generation is known as eye blinks-based authentication, in which the PIN is generated by finding the eye blinks in successive picture frames. This project presents a real-time application that integrates eye blink-based PIN input, face recognition, and OTP to avoid attacks by shoulder surfing and thermal tracking (One Time Password).

Keywords:- *PIN, Shoulder Surfing, Thermal Tracking, Authorization.*

Through the keyboard by physically entering through the keyboard. And one of the attacks used to crack passwords in public locations is the shoulder surfing attack, which uses others standing next to the person entering the password.

By avoiding two methods, we can reduce the majority of password cracking attacks that occur today by implementing three layers of password authentication for logging into any application. Thisproject can be used as a plugin for any application that is being developed, for ATMs, or if we want websites to be securely entered.

I. INTRODUCTION

PIN (personal identification number) or passwords are the one of the most required components in the nowadays world for any software application, websitesand as well as machines which uses the software.

As the usage of the password is increased in almost every application or device, we use the protection to those password is also necessary. Security for those password is very important some of the applications or machines with work on password authentication are like any applications like google-pay, Instagram and machineslike ATM…. these requires an authentication by user by entering the password for performing operation. when user enters the password directly through keyboard in public places or place where the people are present beside you when you entering password which leads to less security where they can crack the password by main two ways, they are shoulder surfing attack and thermal tracking attack.

The thermal tracking and shoulder surfing are the two major types of attacks which are happening for password cracking. The One of the types of attacks used in password cracking is the thermal attack.

The attackers may trace the heat prints on the keyboard and crack the password quickly by using thermal cameras when the user inputs the password For every user to securely login to the system, the Three-Way Authentication System provides three phases, which are as follows: 1) Using the LBPH algorithm for face recognition; 2) Entering passwords in a virtual keyboard by blinking your eyes 3) Input the OTP received on your mobile phone.

The paper consists of different sections in it the basic go-through of it is given as first the paper starts with the abstract main importance of the system followed by the I. Introduction of the system followed by the II. Literature Survey of existing System and drawbacks in it followed by the III. System design which consists of various diagrams which we followed for this system followed by the next section IV. Methodology and results of the system we developed and the next section is V. Conclusion and next section is VI. Future scope and the last section VII. References.

II. LITERATURE SURVEY

There are multiple systems available for user authentication, as well as various methods of Single way authentication, and their descriptions of some similar related systems and their short comings.

- A Paper entitled with “Eye-pass shapes Method” is proposed and developed which is an two way authentication mechanism where the user will authenticate two way manner in Pass-Shape the user must paint shapes that consists of strokes in a certain order. This method increases the comprehensibility but does not give the full qualityof security this is the major drawback in that system.

- Andreas, Florian, and Albrecht (2012) reported "a unique gaze-based authentication technique" on all images that uses a cued-recall graphical pass. Using a computation of visual attention, this approach masks image regions that are likely to be focused on. They created a realistic danger model for assaults in public places, such as tracking a user's behavior when taking money from an ATM.

- Another paper called Heat of the Moment: Characterizing efficacy of Thermal camera -Based Attacks In this paper we have demonstrated a thermal camera-based attack against keypad code entry that is easily scalable and, in many scenarios, quite effective: even a minute after the keypad was pressed, we were till able to recover over half of the entered codes is the drawback of that system.

- A one more paper proposed with the title Drag- and-Type a method which is developed for typing with virtual keyboards on the small touch screens this on small touch screens devices, a more secured password entering in virtual keyboard in small scale devices the drawback of this paper is it is suitable for small screen system only and security is less against spyware attacks.

- A paper Real-Time Eye Tracking using smart camera is similar to proposed system for hands-off gaze-based password entry this system is three steps for authentication but this system has some drawbacks some of them are the accuracy in detecting the face is only 60% and this system is implemented through the smart camera which is little expensive for every system to have smart camera.

III. DESIGN

A. The Design of the System Plays Very Important Role in any System which we Design Requires a Basic Plan before we Start Developing that System the Below Diagram is the Flowchart of the Proposed System where this Diagram is the High-Level Diagram which Shows the Flow of the Project in the Detailed Manner.

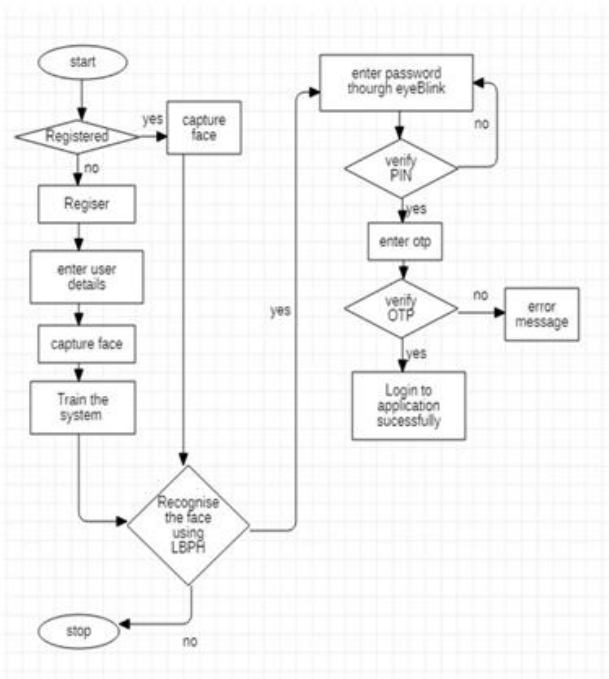

Fig 1. High level flowchart diagram

B. Use-Case Diagram:

The use case diagram is a system design diagram that is prepared to describe the activities users will undertake with the system and how the system will interact with the user. Various interactions between the system and the user are written at the end, and it should meet the user's requirements.

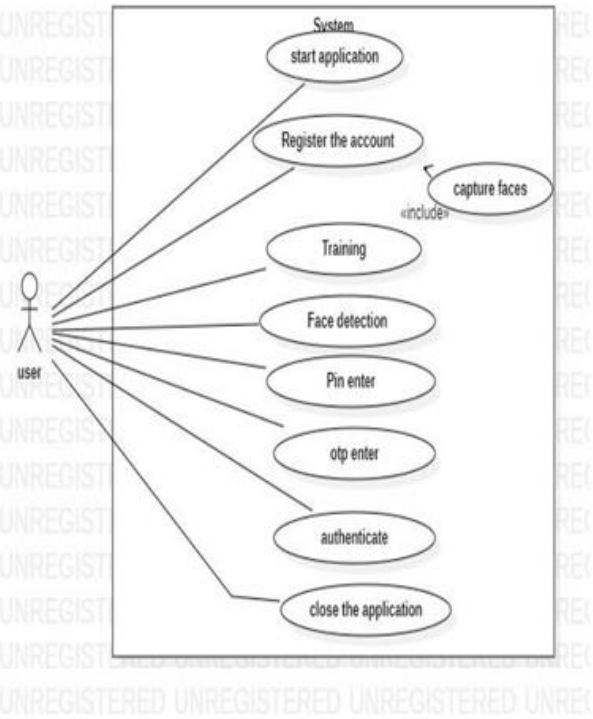

Fig 2. Use-Case Diagram

Figure 2 displays the use-case diagram of the system we are constructing. It has several use-cases where the user would interact with people inside the system, and there is only one sort of user, who is the person who wishes to connect to the system.

IV. METHODOLOGY

The methodology component of any project plays a critical role in the project. This area of the paper outlines how the system was developed and the procedures that were taken during the development process.

Table 1. Major Steps Followed Through Methodology

NO.	STEPS
1	Face Detection using LBPH Algorithm
2	Building Training Model
3	Eye-Blink detection
4	Authentication using OTP

The process followed during the system developed are mainly four sections in it first is face-detection using the LBPH algorithm followed by the building the training model using the faces captured and next is creating a virtual keyboard entering password through eye blinks and last step is the authentication through OTP.

A. Face Capturing Using Haarcascade Classifier:

The Face detection is the first step in the authentication process where as soon as the user while registering enter the details like name, password to set and the mobile number along with that for the Face detection he needs to give his face as input. The Face detection mainly contains two parts in it Mainly the face detection algorithm is implemented by machine learning algorithms called as Haarcascade classifier and LBPH.

The Haarcascade classifier is the one of the object detection algorithm used to identify the faces of the persons using the input as image or video given by them.

*B. Face Recognition Using LBPH***:**

Once the face detection is done by the previous step now the LBPH algorithm will extract the features of the face like jawline, eye like features is extracted and those features were trained using the Train() with the dataset given and results are stored in the trainer file .once the training has done the user clicks on first step for authentication the face will be detected.

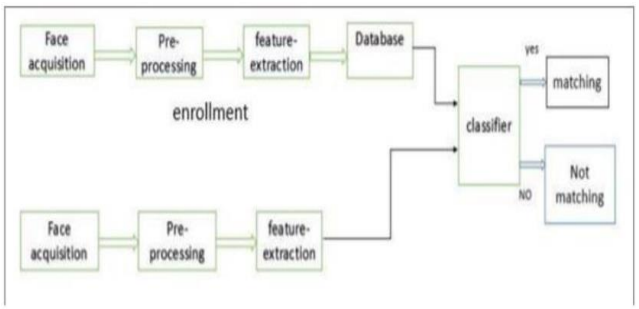

Fig 3. Face recognition block diagram

*C. Eye-Blink Password Using Virtual Keyboard***:**

This is the second step of the authentication process. where it is a major component of the certification Oncethe system detects the face of the If the user enters this stage, the user will enter the password through the eye- blinks as soon as the user as he enters this step, the cameraof the system will turn on. Begin tracking the user's eyes with the use of the LBPH algorithm, where it will take the dark pixels of the user's eye in the face. Once the virtual keyboard starts, there will be 9 digits in It goes from 0 to 9, where the cursor light is. I will be moving from one digit tothe other digit for a In this span of time, each digit cursor will be moving from the first digit to the last digit. This step we have implemented using the OpenCV and DLIB libraries for Eye-Blink detection.

D. Authentication Using OTP:

The OTP is the last third stage in the authentication in the proposed system where the user will receive the OTP to his registered mail-id which is provided while registering here we used the random number OTP generator using feature of python. Once the user receives the password, he will enter the password through the keyboard of system and he logs into the system successfully.

Thus, we successfully able to design the flow of the steps followed in the methodology of the project by completing each step in a very preside manner.

V. RESULTS

The process of methodology is followed each step properly and developed a system with all the Three ways of authentication being done here are the some of the screenshot.

Fig 4. Home Page of the System

The main page of the system we built is shown above. As soon as the user loads the website, the above screen appears. If the user is already registered in, he can click on the facial recognition button. If you are a new user, you may register by clicking the Register button.

Fig 5. Registration Page

If a user is new to the system, he will navigate to the registration page depicted in the picture above, click register, input his email address and password, and mobile number then click add images to provide sample images for facial recognition. Those acquired data will serve as the dataset for the model, and the system will be trained using the captured photographs.

Fig 6. Fist Layer of Authentication

Once the system is given with the images and trained the first layer of authentication face recognition is done ponce registered user clicks on the Face Recognition button.

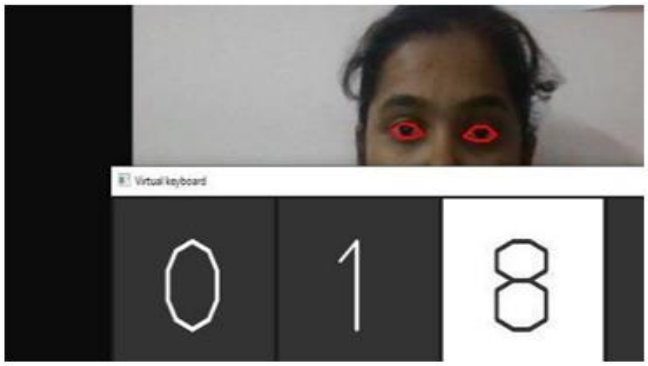

Fig 7. Virtual Eye-Blinking Keyboard

The second step of authentication requires the user to type a password on a virtual keyboard by blinking when the cursor reaches a digit.

VI. CONCLUSION

All three methods of authentication, face recognition, eye- blinking password, and one-time password, are implemented with high precision in face recognition. and accurate results in eye-blinding using a virtual keyboard and obtaining the OTP in the shortest time possible to send an email using the DLIB and OpenCV libraries.

FUTURE ENHANCEMENT

The enhancements that will be made in the near future to the project include the fact that we have now designed the system and implemented it in the web application; in the future, we will be able to implement this system on mobile devices as well; and additionally, we will provide the option of obtaining an OTP for both the email address and the registered mobile number.

REFERNCES

[1]. Weaver, J., Mock, K. and Hoanca, B., 2011. Gaze-based password authentication through automatic clustering of gaze points. 2011 IEEE International Conference on Systems,Man, and Available at:<https://ieeexplore.ieee.org/abstract/document/6084072/>

[2]. Development of Personal Identification Number Authorization Algorithm Using Real- Time Eye Tracking & Dynamic Keypad Generation.\Availableat: <https://ieeexplore.ieee.org/document/9417950>

[3]. Opencv-python-tutorials.readthedocs.io. 2020. Face Detection Using Haar CascadeOpencv-PythonTutorials1Documentation. [online]Availablat:<https://opencv-python tutroals.readthedocs.io/en/latest/py_tutorials/py_objdetect/py_face_detection/py_face_detection.html> [Accessed 12 November 2020].

[4]. Medium 2020. Face Recognition: Understanding LBPH Algorithm. [online] Available at: <https://towardsdatascience.com/face- recognition-how-lbph-works-90ec258c3d6b> [Accessed 12 November 2020].

[5]. Hackaday.io 2020. Eye Blink Detection Algorithms | Details Hackaday.Io .[online]Available<https://hackaday.io/project/27552-blinktotext/log/68360-eye-blink- detection-algorithms> [Accessed 12 November 2020].

[6]. Rosebrock,A., 2020. Eye Blink Detection with Opencv, Python, And Dlib-Pyimagesearch. [online] PyImageSearch. Available at: <https://www.pyimagesearch.com/2017/04/24/eye-blink-detection- opencv-python-dlib/> [Accessed 12 November 2020].

[7]. FreeCodeCamp.org. 2020. How Time-Based One-Time Passwords Work And Why You Should Use Them In Your App... [online] Available at: <https://www.freecodecamp.org/news/how-timebased-on time-passwords-work-and-why-you-should-use-them-in-your- app- fdd2b9ed43c3/> [Accessed 12 November 2020].

[8]. En.wikipedia.org.2020. Time-Based One-Time Password Algorithm. [online] Available at: <https://en.wikipedia.org/wiki/Time- based_One-time_Password_algorithm> [Accessed 12 November 2020].

[9]. Mehrubeoglu, M., Linh Manh Pham, Hung Thieu Le, Muddu, R. and Dongseok Ryu, 2011. Real-time eye tracking using a smart camera. 2011 E Applied Imagery Pattern Recognition Workshop (AIPR).

[10]. Mehrubeoglu, M., Ortlieb, E., McLauchlan, L. and Pham, L., 2012. Capturing reading patterns through a real-time smart camera iris tracking system. Real-Time Image and Video Processing 2012.

[11]. Kiruthika, K., 2016. A Secure Pin Authentication Method against Shoulder Surfing Attacks. International Journal of Engineering And Computer Science.

[12]. Kwon, T., Na, S. and Park, S., 2014. Drag-and-type: a new method for typing with virtual keyboards on small touchscreens. IEEE Transactions on Consumer Electronics, 60(1), pp.99-106.