iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VI Month of publication: June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35344

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Eye Tracker for Password Authentication

Archana M Barki[1], Bhuvana M C[2], Namratha Prabhu[3], Rashmi Gopala Bhat Saranga[4], Prof. Chetan Umadi[5]
[1, 2, 3, 4, 5]Department of Telecommunication Engineering, Dayananda Sagar College of Engineering

Abstract: In today's quickly expanding digital environment, security is one of the most important worries that everyone has. Personal Identification Numbers, or PINs, are used to address security issues. Password authentication with PINs, on the other hand, requires clients to physically enter the password, which can be cracked via heat monitoring or thermal tracking. Hands-off gaze-based password or PIN entering techniques used in password or PIN authentication leave no physical traces and so provide the highest level of security for the password or pin entry. Gaze-based authentication entails tracking the eye center and examining the client's gazes for password entering and finding the position of eyeballs across sequential frames of the image. The term "eye detection" refers to the detection of eye characteristics in a single frame. The method of measuring and correlating the positions and movements of the eyes is known as eye-tracking. Blinking ratio of the eye is used for entering the password which will then be compared with the original password for authentication process.
Keywords: PIN (Personal Identification Number), gaze-based, eye detection, eye tracking, Blinking ratio.

I. INTRODUCTION

Human-computer interaction (HCI) is concerned about how humans and computers interact in work and communication. Inputs and outputs are two aspects of this information exchange. Everyone often use an automatic all-pin verification system that provides privacy and security. The security of the cash management system on Automatic Teller Machines (ATMs) of banks can be achieved with PINs (Personal identification numbers). PINs are used to accept electronic transactions, unlocking devices and open doors.

According to European ATM Security, fraudulent attacks on ATMs are increasing every year [2]. The fact that the licensed user must enter the code in public places makes it possible to crack the password by thermal tracking or shoulder surfing [2]. This function uses a smart camera, which is used to insert and identify visual-based PINs using real-time eye-tracking.

This proposed system uses the Open cv and image processing techniques to track the eye and record the location of the eye center. Data processing and collection can be achieved with an intelligent camera. The physical password entry will reduce the vulnerability of the authentication process [2].

To overcome this problem an additional layer of security can be added to the system with unsupported authorization of contacts. There are 3 main problems with this tracking technology they are- difficulty in tracking system, complex tracking skills, and user experience.

The main contribution of our work over other proposed strategies is as follows:

- Proposed work will create the most complete, easy-to-use and inexpensive version compared to the existing password authorization systems. In the proposed work, the Eye tracker is very small, lightweight, and usable. Includes real-time viewing positions based on eye movement.
- Proposed work uses a special type of display that is used as a viewing device close to the tracking system, which is much better than large custom display devices such as computers that monitor TVs and projectors.
- This application can be installed on any new pin installation applications. The program currently uses a 9-digit keypad which can also be extended to achieve higher security.

The purpose of this study is to make the face detection algorithm more secure by making it more resistant to tracing attacks, such as shoulder surfing or thermal tracking. Verifying the PIN authentication using the PIN entry without manual detection does not leave the physical marks and thus provides another secure way to enter the password.

Detecting eye movements using consecutive image frames and monitoring the eye centre over time is called authenticity based on visual acuity. This paper introduces real-time application for visualized PIN input, as well as eye detection and tracking of PIN recognition using a smart camera.

II. LITERATURE SURVEY

A. Eye Tracking using Gaze Pin Entry for Password Authentication

Pavitra S R et al [1], Proposed a work in which a gaze based authentication system is introduced where one can enter the pin without entering the pin manually (handoff gaze based pin). The client will select the pin numbers by their eyes with simply concentrating on the digits which is showed on the screen, this method is called as eye gaze or eye tracking. It is characterized by the methodology of recognizing the eye position through video. This gaze model is authentication model which can also be used in cloud computing and virtualization environment. The main intention of this work is to prevent perception attacks during passage of the pin while holding a similar work process that users are associated with and with less extra equipment expenses. This prototype can be consolidated handily with current plans such as ATMs and for the purpose of exchange frameworks. A structure is built to utilize an eye track gadget to avoid thermal tracking assaults and licensed users to go through their password pin with no frenzy of person watched. But there are some limitations associated with this work; proposed method cannot be adjusted to new platforms.

B. Real-Time Eye Tracking for Password Authentication

M. Mehrubeoglu et al [2], This paper presents a model in which the camera is located right above the keypad screen with camera lens directly viewing the user's eye. The smart camera contains a dual processor permits the camera to work well with applications such as pattern matching, optical character recognition and data matrix code in real time. The eye detection algorithm processes about seven frames per second. The camera frame rate specification is not very stringent for this application, since the user pauses over each digit for several seconds. This type of gaze-based PIN entry involves the user entering the PIN code by looking at the PIN pad. The user stares at each digit of the PIN for a few seconds, sequentially moves to the next digit with his/her eyes. The eye tracking application is stopped when PIN entry is completed. Eye detection begins with training the algorithm. This is accomplished by capturing a single frame of the user's eye and saving it as the eye template, The coordinate system conversion is accomplished to standardize the coordinates of the reported eye location, to allow capturing eyes at various angles based on the tilt of the head. From the best matched eye image, iris of the eye is detected using circle or oval matching via edge detection and Hough transforms.

C. Etracker: A Mobile Gaze-Tracking System with Near-Eye Display Based on a Combined Gaze-Tracking Algorithm

Bin Li et al [3], This proposed work introduces a mobile gaze-tracking system with an eye viewing device and tracking algorithms. This system is proposed using the mean value of pupil centres to optimize the changes caused by rapid involuntary movements of the eyes in calibration algorithms. The main handouts of this work are: it is an efficient prototype, inexpensive system which is easy to use. Compared to other gaze-tracking systems, this prototype is small, lightweight, modest and user-friendly. This system computes gaze position in real time by recording eye movement. Based on CNNs (ResNet-101) and a geometric model a combined gaze estimation method is proposed. Compared to other gaze-tracking systems, this prototype is small, lightweight, modest and user-friendly. This system computes gaze position in real time by recording eye movement. But this system has some limitations; in this screen size affects the precision within the clusters and it must be calibrated.

D. Small-Object Smart Eye-Tracking System

Aniwat Juhong et al [4], This paper aims to investigate the creation of an eye tracking system for controlling an electric wheelchair and other appliances, as well as communicating with caretaker via smartphone. This effort was mostly focused on the elderly and crippled. The main goal of the proposed work is to create a prototype of a smart eye-tracking system that can control home appliances, drive an electric wheelchair, and transmit text messages to the caretaker.This work used an image processing module, which is the main module of the proposed system that starts with a webcam that is installed on the eyeglass and also captures the eye image and sends it to a Raspberry Pi for image processing, which is primarily based on C++ with Open CV to obtain the position of the eye ball and also to define eye blink. The cursor control on the Raspberry Pi screen is also controlled by eye movement, which is used to enter commands. For smart eye tracking systems, eye movement and blinking were used as controlled user interfaces. However, this system has significant limitations; it can be used for normal operational behaviour to communicate with a computer by emulating mouse and keyboard.

III.METHODOLOGY

A. Required Tools

1) Python: It is a versatile object-oriented programming language which could be used to create a wide range of applications. Python is released under an OSI-approved open source license that allows consumer applications to use that for free. Python is used for implementation of the proposed methodology.

2) Open CV: (Open Source Computer Vision Library) is a free software library for computer vision and machine learning. Open CV was created to provide a shared infrastructure for computer vision applications and to help commercial products incorporate machine perception more quickly. Open CV was developed to have a common infrastructure for image processing applications and to help commercial applications incorporate machine perception more quickly [13].

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

B. Steps Involved

Step1: Start the camera, then continuous pictures, or video, of the user in front of the camera are captured using a web camera.

Step2: Open CV receives the captured image from the USB camera.

Step3: From the received image it extracts the face and then it is sent to eye detection module which extracts eye region of interest.

Step4: Window location is sent to the feature detection system, and the output will be the co-ordinates of the eye area.

Step5: Finally, the eye tracking module can monitor eye movements to calculate the gaze ratio and detect eye blinks to calculate the blinking ratio.

Step6: Passwords are entered using Eye blinks, and entered passwords compared with original password for verification.

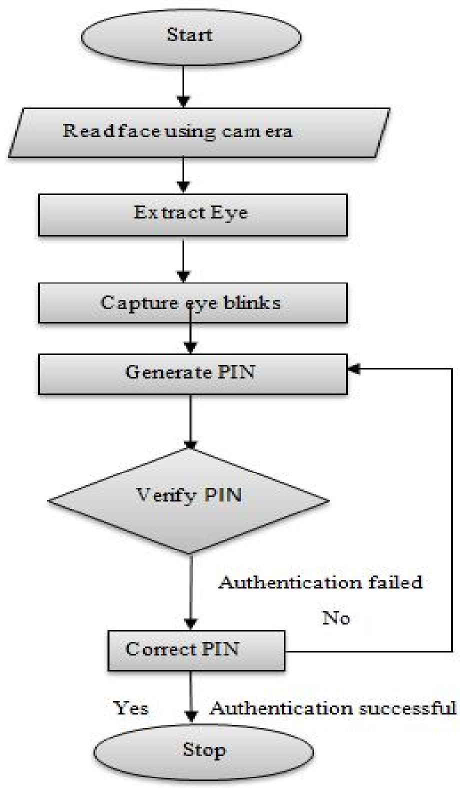


Fig.1 Flow Chart of the steps involved in this method

C. Haar Cascade Algorithm for Face and Eye Detection

This is an Object Detection Algorithm which is used to recognize faces in images or real-time videos. This algorithm is trained using large set of positive images which contains face region and also large set of negative images without any face region. This module takes the images captured using USB camera of the previous module as input and gives the face and eye region as output.

Some of the concepts related to Haar cascade algorithm are shown here.

1) Haar Feature Selection: The digital image features used in image recognition are known as Haar like Features. Haar features, as seen in the image below, are used for extraction of face region.

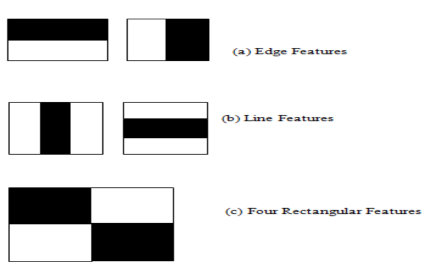


Fig.2 Three types of Haar Features

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

2) Creating an Integral Image: Integral images have pixel values that are the sum of all previous pixel values at each (x, y) location. The following explanation will assist in completing the task.

5	4	3	8	3
3	9	1	2	6
9	6	0	5	7
7	3	6	5	9
1	2	2	8	3

5	9	12	20	23
8	21	25	35	44
17	36	40	55	71
24	46	66	76	101
25	49	61	89	117

Fig.3 5 ×5 Matrix representing the Pixels of an Image and its integral image

Average intensity over the highlighted area of normal image is calculated as follows.
9 + 1 + 2 + 6 + 0 + 5 + 3 + 6 + 5 = 37 37 /9 = 4.11
To do this totally 9 operations are required. So for 100 such operations, multiply 100 by 9 to get 900 operations.
(76 – 20) – (24 – 5) = 3737 / 9 = 4.11
This required four operations in total. We'd need 56 + 100 * 4 = 456 operations to complete 100 such operations. Using an integral image requires around 50% less computations for a hundred operations over a 55 matrix. Consider how much of a difference it makes when it comes to photos and other similar procedures. Creation of an integral image changes other sum difference operations by almost O(1) time complexity, thereby decreasing the number of calculations.It simplifies the calculation of the sum of pixels—no matter how large the number of pixels—to an operation involving just four pixels. Nice, isn't it? It makes things superfast.

3) Ada Boost Training: This process selects only those features known to improve the predictive power of the model, reducing dimensionality and potentiality improving execution time as irrelevant features need not be computed. During this window of the specific size is moved over the image and for each sub section of the image the Haar features are calculated. The difference is then compared to a learned threshold that separates non-object from objects.

4) Cascading Classifiers: It consists of collection of storage, where each storage is an ensemble of week learners. The week learners are simple classifiers called decision stumps. Each stage is trained using a technique called boosting. Boosting provides the ability to train a highly accurate classifier by taking a weighted average of the decisions made by the weak learners. While the window slides, it detects whether the region is positive or Negative. If the positive region is detected then it considers that the object is found and passes it on to the next stage. If the negative region is detected then the sliding window considers the next smaller region of the image. After the classifier passes the region to the next stage. The detector reports an object found at the current window location when the final stage classifies the region as positive.

D. Feature Extraction

The window location from the above module is considered to detect the key facial structure of the in face and locate the facial structures with the specific (x, y) co-ordinates values. Then the co-ordinate values of the left and right eyes are considered and the polygon is drawn over the eye region. Facial land mark detector is used to achieve this process.

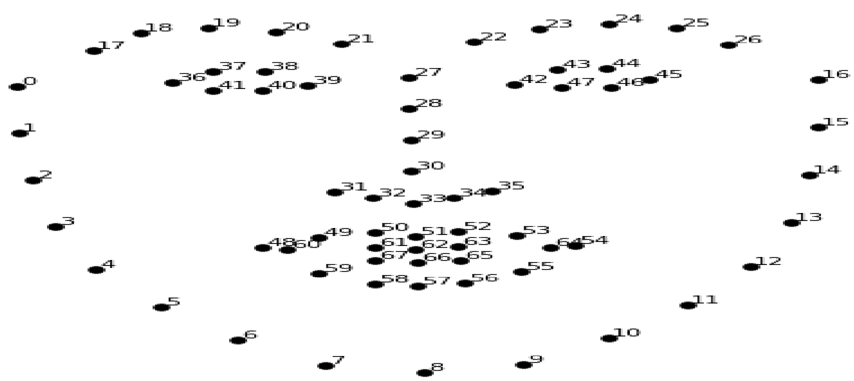


Fig.4 Facial Landmarks

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

	X	Y		X	Y
36	403	321	42	495	320
37	415	313	43	508	311
38	430	313	44	521	311
39	443	326	45	533	316
40	430	326	46	523	321
41	415	326	47	509	322
Left Eye Values			Right Eye Values		

Fig.5 pixel values for drawing polygon over the eye region

Based on the above pixel values the polygon is drawn over the eye region which is shown in Fig. 7.

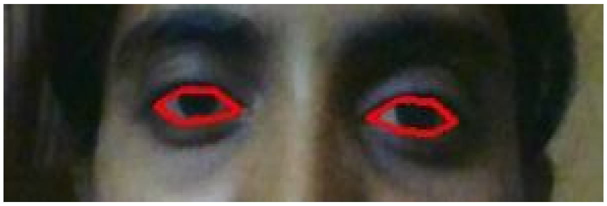


Fig.6 Polygon Drawn over the eye region

E. Eye Tracking

Virtual keyboard will be displayed when we open eye-tracking module. The eye blinking ratio will then be determined, and the appropriate letter will be selected as the password.

Blinking Ratio Calculation:

Step 1: The first step is to gather information. The values of the ocular region's coordinates are used as input.

Step 2: Get the left eye's horizontal and vertical lines.

a. Find the midpoint of the 37th and 38th coordinates, as well as the 40th and 41st.
b. Join the points to the vertical line.
c. Join the 36th and 39th point to get the horizontal line.

Step 3: Obtain the horizontal and vertical of righteye:

a. Calculate the midpoint of 43rh, 44th co- ordinate as well as the 46th and 47th Join the points to the vertical line.
b. Join the points to the vertical line.
c. Join the 42th and 47th point to get the horizontal line.

Step 4: Calculate the Blinking Ratio:

a. Blinking Ratio of left eye:
b. Blinking ratio of left eye = length of the horizontal line/ length of the vertical line.
c. Blinking Ratio of right eye: Blinking ratio of right eye = length of the horizontal line/ length of the Vertical line
d. Blinking ratio = (Blinking ratio of left eye + blinking ratio of right eye) / 2 [14].

Step 5: Initialize the Blinking frames to 6.

If Blinking ratio >=5
Increase the blinking frames value by one
Else
Do nothing

Step 6: If Blinking frames >=6, then update the letter as password.

All the passwords are entered using above steps and it is stored in the array, and then it's compared with original password for authentication purpose.

IV. RESULTS

A. Step 1: Click on "Click Here" option to open Eye Tracking System.

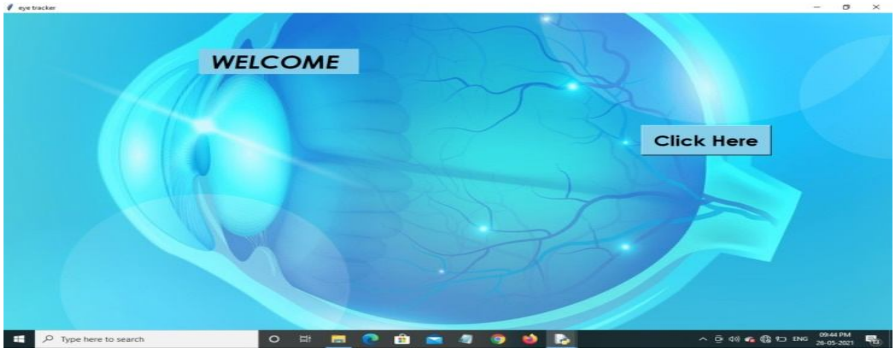


Fig. 7 Welcome Page

B. Step 2:

a. Click on face capturing for collecting continuous image frames.
b. Train the Eye Tracking Module using captured image frames.
c. Click on Face Recognition and Password Detection for opening Virtual Keyboard.
d. Click on Quit option for quitting Eye Tracking module.

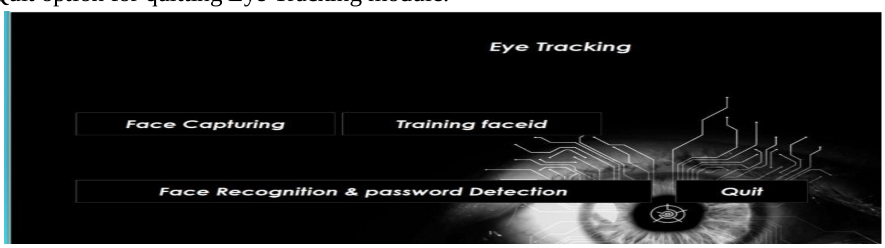


Fig. 8 Eye Tracking Module

C. Step 3: Virtual Keyboard is opened for entering password.

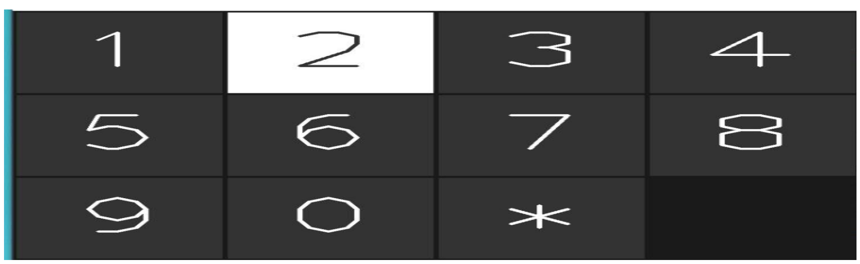


Fig. 9 Virtual Keyboard (Curser on digit 2)

D. Step 4: Enter the Password Using Eye Blinking.

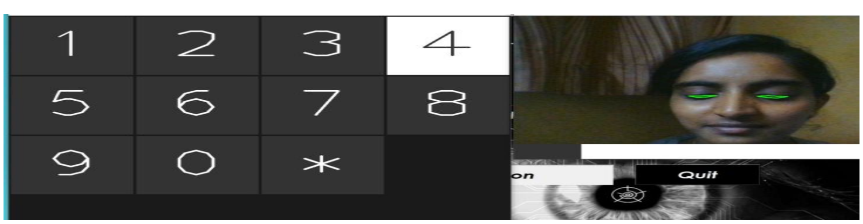


Fig.10 Password Entry Using Eye Blinks

E. Step 5: Displaying of authentication message.

a. When the entered password is correct display a message saying that "password matched".

```
1.0
1.0
1.0
1.0
1.0
text1 ['3', '4']
3 4
Enter password
<class 'str'>
password matched
```

Fig. 11 Screenshot of Password Matched

b. When entered password is incorrect display an error message saying that “Not matched”.

```
text1 ['1', '2']
1 2
Enter password
<class 'str'>
not matched
```

Fig.12 Screenshot of Password not matched.

V. CONCLUSION

A smart-camera based eye-tracking device has been incorporated as a new application for gaze-based PIN recognition. The system has been successfully tested with numbers, and it could be expanded to handle character and digit password combinations in the future. The user password is protected from assaults like shoulder surfing and thermal monitoring, and it's especially handy for persons who are physically impaired. The user's gaze stability affects the precision of the detected PINs, which must be taken into account. PIN identification is currently conducted after real-time eye tracking and eye centre computations and recordings have been completed. This method can be further developed for usage in camera-based devices such as mobile phones, laptops, and desktop monitors. This is the most secure solution for the future, and it is extremely beneficial to all sectors of the corporate world. By incorporating additional enhancements at higher levels, the proposed system can be used for high-level security systems. In the future, gaze-based password entry could be expanded to include mobile phones and other camera-based systems, as well as ATMs.

REFERENCES

[1] Pavitra S R , Pushpalatha S, 2020, “Eye Tracking using Gaze Pin Entry for Password Authentication”, *International Journal of Engineering Research & Technology (IJERT)* Volume 09, Issue 06 (June 2020).

[2] M. Mehrubeoglu and V. Nguyen, "Real-time eye tracking for password authentication," *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1-4, doi: 10.1109/ICCE.2018.8326302.

[3] Bin Li, Hong Fu, Desheng Wen and Wailun LO, “Etracker: A Mobile Gaze-Tracking System with Near-Eye Display Based on a Combined Gaze-Tracking Algorithm”. *Sensors (Basel)*. 2018 May 19; 18(5):1626.doi: 10.3390/s18051626. PMID: 29783738; PMCID: PMC5981618.

[4] Aniwat Juhong, C. Pintavirooj, T. Treebupachatsakul “Smart Eye-Tracking System”, *International Workshop on Advanced Image Technology 2018 (IWAIT)*, Chiang Mai Thailand, 2018.

[5] Nuri Murat Arar, Jean-Philippe Thiran, “Robust Real-Time Multi-View Eye Tracking” Student Member and Senior Member, IEEE, 3 Jan 2018.

[6] R. Bama and R. Revathy “Advanced Safe PIN-Entry against Human Shoulder-Surfing,” IOSR Journal of Computer Engineering, e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. II (July – Aug. 2015), PP 09-15.

[7] Garcia-Zapirain, Lopez-Basterretxea, Mendez-Zorrilla, “Eye/head tracking technology to improve HCI with iPad applications. Sensors” 2015.

[8] P. Marlin, Mayberry, Hu, Salthouse, Ganesan, “Design of a wearable, real-time mobile gaze tracke.” *In Proceedings of the 12th annual international conference on Mobile systems, applications and services*, Bretton Woods, NH, USA, 16–19 June 2014.

[9] Mehrube Mehrubeoglu, Evan Ortlieb, Lifford Mclauchlan, Linh Manh Pham. “Capturing reading patterns through a real-time smart camera iris tracking system”. SPIE 8437, Real-Time Image and Video Processing 2012, 843705, Jun 2012, Brussels, Belgium. ff10.1117/12.922875.hal-01233270.

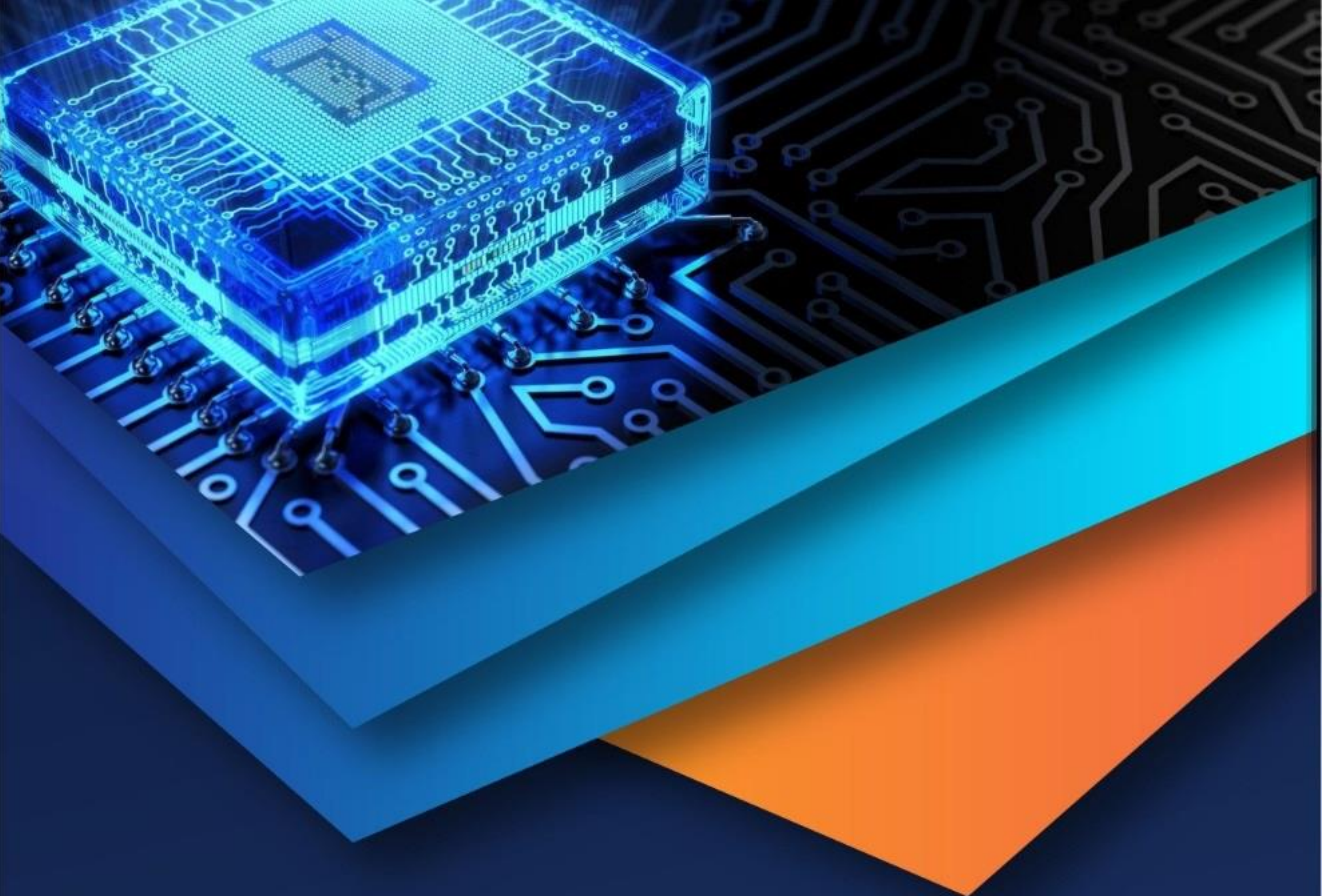
[10] LinhManh Pham, MehrubeMehrubeoglu, Hung Thieu Le, RamchanderMuddu, and DongseokRyuTexas “Real-Time Eye Tracking for Password Authentication” A&M University-Corpus Christi, School of Engineering and Computing Sciences Corpus Christi, Texas, USA,2011.

[11] K. Mock, J. Weaver, and B. Hoanca, “Gaze-Based Password Authentication through Automatic Clustering of Gaze Points,” *Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics*, Oct. 2011.

[12] K. Mowery, S. Meiklejohn and S. Savage, “Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks,” WOOT ’11, pp. 1-8, August 2011.

[13] Gitam University Student Paper

[14] Delhi Technological University student Paper



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429