Three Layer Password Authentication Using Eye Blink

Chidanandan V[1], Aishwarya[2], Gagana C M[3] , Maheshwari[4] , Monisha G[5]
[1]Assistant Professor, Dept of CSE
[2, 3, 4, 5]Dept of CSE
[1, 2, 3, 4, 5] Dr Ambedkar Institute of Technology, Bangalore-560056

Abstract- *Personal identification numbers (PINs) play a crucial role in user authentication and security measures. However, traditional password authentication methods that rely on PIN entry using physical means are susceptible to password cracking techniques like shoulder surfing or thermal tracking. To overcome these vulnerabilities, this project introduces a novel approach utilizing hands-off eye blink PIN entry techniques, which ensures a more secure method of password input. By leveraging eye blinks as a form of authentication, this technique eliminates physical footprints, enhancing the overall security of the system. Moreover, this project incorporates real-time applications by integrating eye blink-based PIN entry with face detection and the utilization of One Time Passwords (OTPs). This combination offers a robust defense against shoulder surfing and thermal tracking attacks, significantly enhancing the security and reliability of the authentication process.*

I. INTRODUCTION

One of the crucial security prerequisites for authentication systems in general terminals is to ensure a seamless, rapid, and robust user experience. As individuals encounter authentication mechanisms on a daily basis, conventional knowledge-based approaches like passwords fall short in terms of safety. Malicious observers exploit surveillance techniques such as shoulder-surfing, wherein they clandestinely capture users' authentication data by observing their keystrokes. Furthermore, security issues arise due to inadequate user-system interactions. In response to these challenges, researchers have proposed the adoption of eye tracking systems, enabling users to enter their passwords by gazing at suitable symbols in a designated sequence. This innovative approach renders users impervious to shoulder-surfing attacks. Leveraging eye movement tracking as a natural and intuitive interaction method, security systems based on this technology offer a promising solution to enhance both system security and usability. Consequently, the primary objective of this paper is to critically evaluate various techniques and solutions for effectively incorporating eye movement tracking within security systems.

II. EXISTING SYSTEM

There is sample related work in the fields directly related to this project.

Alexander, Martin and Heinrich (2009) present “Eye-Pass Shapes Method”, Eye Pass Shapes extends and develops two authentication approaches via combining them, Pass Shapes and Eye PIN. In Pass Shape the users must paint shapes (that consist of strokes) in a certain order, this method increase memorability but doesn’t improve security in comparison with PIN or password entry. Eye PIN is focused on security instead of usability.

The user’s PIN is still the token of authentication, and the security is improved when the input method is changed. Rather than inserting numbers, an eye movement is performed by the user representing the associated digits. Eye-Pass Shapes can be considered simpler to be detected than the exact location of the user's look and can work with cheap devices.

Alain, Sonia and Robert (2010) present “CGP enhancements”, CGP which is an abbreviation for Cued Gaze Points can be considered as a system of graphical pass-word defending from such attacks with the use of eye-gaze pass-word input, rather than mouse-clicks, but it requires certain approaches for improving the accuracy of gaze. This study presented two improvements: a nearest-neighbor gaze-point aggregation method and a one-point calibration prior to entering the pass-word. They reached the conclusion that those improvements made a significant enhancement to the precision of users’ gaze and system efficiency.

Justin, Kenrick and Bogdan (2011) present “Eye Dent System”, which is an improvement to the present authentication systems that depends on eye-tracking which requires pressing a trigger by the user when looking at any symbol. Rather than that, Eye Dent, gaze points are being clustered in an automatic way for determining the character chosen by the user; this method is beneficial in allowing the user the authentication at their preferred pace, instead of a predetermined dwell time. In addition, not having visible trigger does not reveal the number of symbols in the password.

Andreas, Florian and Albrecht (2012) presented “a novel gaze-based authentication scheme”, this scheme uses cued-recall graphical pass-word on all images. This approach uses a computation of visual attention for masking these image parts which will probably be focused on. They created a realistic threat-model concerned with the attacks which could happen in public places, like recording user’s actions throughout the process of drawing money from an ATM.andreas, Florian and Albrecht (2012) presented “a novel gaze-based authentication scheme”, this scheme uses cued-recall graphical pass-word on all images. This approach uses a computation of visual attention for masking these image parts which will probably be focused on. They created a realistic threat-model concerned with the attacks which could happen in public places, like recording user’s actions throughout the process of drawing money from an ATM.

David Rozado (2013) present “the subject specific gaze estimation parameters” using this parameter which has been gathered throughout a calibration process to render impractical to another individual to input a password by gazing even in the case where the impostor is aware of the correct password. Mihajlov, Trpkova and Arsenovski (2013) present “eye tracking study of Image Pass”, ImagePass can be considered as a graphical authentication system that is based on recognition. The aim of the study was discovering the users perception and reaction to graphical authentication. Mohamed, Florian, Mariam, Emanuel, Regina and Andreas (2016) present “Gaze TouchPass Scheme”, it’s a multimodal method combining touch and gaze regarding shoulder-surfing resistant authentication in mobiles. GazeTouchPass accepts pass-words with several switches between input modalities throughout the process of authenticating.

Zhenjiang, et al. (2017) present “iType System”, a system which utilizes eye gaze to type private input on commodity mobile platforms.

III. PROPOSED SYSTEM

Introducing a novel approach, our system incorporates computerized vision technology to generate a secure Personal Identification Number (PIN) based on eye blinks. By employing a combination of methodologies such as face and eye detection, eye blink detection, rectangular and circular pupil edge detection, and eye tracking, our system ensures robust security.To initiate the process, the system acquires images captured by a USB web camera. Subsequently, it employs a Haar Cascade classifier to detect faces and eyes. Then, an eye blink detection method utilizing the Histogram of Oriented Gradients (HOG) algorithm determines whether an eye is open or closed. By accurately detecting the eye region of interest, the system crops it and proceeds to identify all potential circles within that area, thereby achieving precise eye pupil detection. In order to provide enhanced security for user accounts, our proposed system employs a three-level authentication mechanism. Firstly, it utilizes face recognition using the Local Binary Patterns Histograms (LBPH) algorithm. This ensures that only authorized individuals gain access to the system. Secondly, the system generates a password based on eye blinks, leveraging the secure and unique characteristics of each user's eye movements. Finally, an additional layer of security is added through One-Time Password (OTP) verification, which requires users to provide a unique code sent to their registered mobile devices.

By combining these three levels of authentication, our system establishes a robust and multi-faceted approach to safeguarding user accounts. This unique combination of eye blink-based PIN generation, face recognition, and OTP verification ensures a high level of security and significantly reduces the risk of unauthorized access.

SCOPE OF THE PROJECT --In recent research, eye tracking systems have emerged as a promising solution for enhancing system security and usability by allowing users to enter passwords through gaze-based interactions, eliminating the vulnerability of shoulder surfing. By leveraging the natural behavior of eye movements, these systems enable users to select symbols in the correct order by simply looking at them. This paper aims to provide a comprehensive review of various techniques and solutions pertaining to eye movement tracking in security systems.Eye tracking, as a natural interaction method, holds significant potential in the field of system security. By tracking and analyzing eye movements, these systems can authenticate users based on their unique gaze patterns, providing a more secure alternative to traditional password-based authentication methods. Moreover, since eye tracking is an inherent behavior, users find it intuitive and user-friendly, enhancing the overall usability of security systems.

PROBLEM STATEMENT OF THE PROJECT--Personal Identification Numbers (PINs) have become a widely adopted method for user authentication in various applications, including ATM transactions, electronic transactions, device unlocking, and access control systems. However, ensuring flawless identity authentication remains a significant challenge, even when PIN authentication is implemented. This is particularly evident in financial systems and gate access control, where the risk of fraudulent activities is prevalent. To shed light on the severity of the issue, European ATM Security reports a staggering 26% increase in fraud attacks on

ATMs in 2016 compared to the previous year. This alarming statistic highlights the pressing need for improved security measures in PIN entry processes.

IV. LITERATURE REVIEW

In a project report, a literature survey or literature review serves to explore and analyze existing research and analyses conducted in the field of interest. It provides an overview of the current knowledge, including significant findings, theoretical contributions, and methodological advancements related to the topic. By considering various parameters and the scope of the project, the literature survey aims to understand the background of the project and identify flaws or unsolved problems in the existing system.

The literature survey delves into a scholarly paper that incorporates secondary sources, such as academic-oriented literature, theses, dissertations, and peer-reviewed journal articles. It offers a comprehensive examination of prior work before presenting the methodology and results of the project. The literature review is often a critical component of research proposals or prospectuses, as it contextualizes the study within the existing body of literature and provides valuable insights for the reader.

The main objectives of a literature survey are to situate the current study within the broader context of existing research and to provide a comprehensive understanding for the reader. It covers a range of materials, including universally accepted theories, both generic and specific books on the topic, and a chronological review of research conducted in the field, from oldest to latest. Furthermore, the literature survey identifies challenges and ongoing work in the field, if available, offering a deeper understanding of the existing problems that motivated the proposed solutions in the project.
By examining the existing work on the given project, the literature survey aims to address the problems associated with the existing system and provide the reader with knowledge on how to tackle these issues and offer potential solutions.

In summary, a literature survey is a crucial component of a project report that investigates existing research and analyses related to the project's topic. It helps uncover flaws in the existing system and guides the project towards addressing unsolved problems. By exploring accepted theories, published books, chronological research, and ongoing work, the literature survey provides a comprehensive overview of the existing work and sets the foundation for further investigation and proposed solutions.

V. REQUIREMENT SPECIFICATIONS

FUNCTIONAL REQUIREMENTS

This section outlines the functional requirements of the system, expressed in a natural language style:

1. Develop a web application using the Flask framework to facilitate the system's functionality.
2. Implement a user registration feature that allows users to create their accounts within the system.
3. Enable the system to collect facial images from users and utilize the Local Binary Patterns Histograms (LBPH) algorithm to train and store the facial recognition model.
4. Utilize the LBPH algorithm to accurately recognize and authenticate users' faces during the login process.
5. Implement a feature that generates a password based on the user's eye blinks, leveraging the Haar cascade classifier.
6. Enable the system to authenticate users using a combination of their Personal Identification Number (PIN) and user ID. Once verified, the system should generate and send a One-Time Password (OTP) to the user for further authentication.
7. Implement an OTP authentication mechanism, where users are required to enter the received OTP to complete the authentication process.
8. Ensure that the application efficiently and securely authenticates users by employing all three levels of authentication (face recognition, eye blink-based password, and OTP verification) to provide robust security for their accounts.

NON FUNCTIONAL REQUIREMENTS

In addition to the functional requirements, the system must also adhere to certain non-functional requirements. These requirements define constraints and qualities that the system should possess. Here are some non-functional requirements for the system:

1. Portability: The program should be self-contained, allowing it to be easily moved from one computer to another. It is assumed that the program will be used in environments with network connectivity.
2. Capacity, Scalability, and Availability: The system should aim for 100% availability at all times. It should be designed to handle a growing number of clients and volunteers, ensuring scalability to accommodate additional users without compromising performance.
3. Maintainability: The system should be optimized for supportability and ease of maintenance. This can be

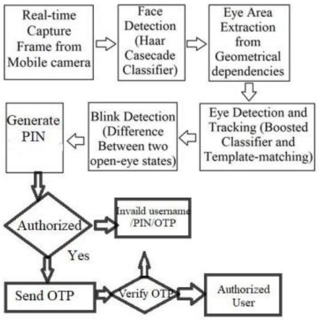
achieved through the use of documentation, coding standards, naming conventions, class libraries, and abstraction techniques. These practices will facilitate future updates, bug fixes, and enhancements to the system.

4. Security: The system should prioritize security measures to protect user data and prevent unauthorized access. This includes encryption of sensitive information, secure communication protocols, and adherence to industry best practices for data protection.
5. Performance: The system should be designed to deliver efficient and responsive performance. It should be able to handle multiple concurrent requests without significant degradation in response times. Performance optimization techniques, such as code optimization and database indexing, can be employed to achieve this goal.
6. Usability: The system should be user-friendly and intuitive, ensuring ease of use for both clients and volunteers. User interfaces should be designed with clear navigation, proper feedback, and appropriate error handling to enhance the overall user experience.
7. Compatibility: The system should be compatible with different operating systems, web browsers, and devices. It should be responsive and adaptable to various screen sizes and resolutions, enabling users to access and interact with the system seamlessly across different platforms.

By addressing these non-functional requirements, the system can provide a robust and reliable user experience, ensuring portability, scalability, maintainability, security, performance, usability, and compatibility.

VI. SYSTEM DESIGN

SYSTEM ARCHITECTURE


Real-time Capture Frame from Mobile camera
Face Detection (Haar Casecade Classifier)
Eye Area Extraction from Geometrical dependencies
Eye Detection and Tracking (Boosted Classifier and Template-matching)
Blink Detection (Difference Between two open-eye states)
Generate PIN
Authorized
Invaild username /PIN/OTP
Yes
Send OTP
Verify OTP
Authorized User

Top level overview, showing work flow of eye blink PIN authentication System.. We are recognize the face using LBPH and capture the eye blinks using HAAR cascade eye detection, Authenticating user id and PIN once PIN is valid system will send OTP to the user mobile number and validate.

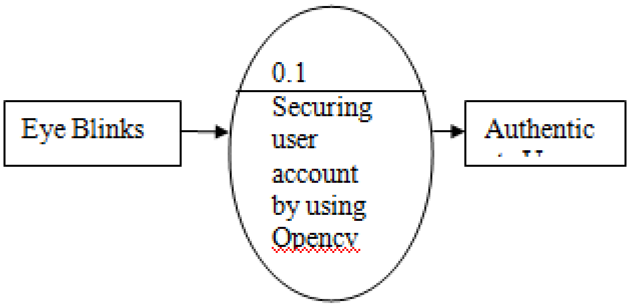
DATA FLOW DIAGRAMS

A data-flow diagram (DFD) is a visual representation that illustrates the flow of data within a process or system, typically an information system. It provides insights into the inputs, outputs, and interactions of entities and processes involved. Unlike control flow diagrams, DFDs do not depict decision rules or loops. Instead, they focus on the flow of data. DFDs serve as valuable tools in structured analysis and data modeling. In the context of UML (Unified Modeling Language), activity diagrams often fulfill a similar role as DFDs. However, a variant of the DFD known as a site-oriented data-flow plan can be used in specific scenarios.

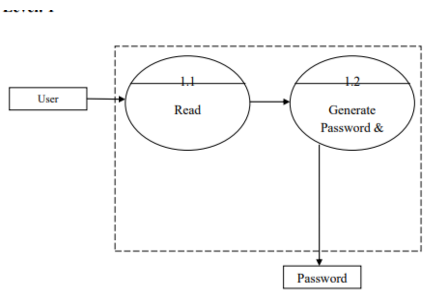
A site-oriented data-flow plan is a specialized form of a DFD that emphasizes the flow of data within a specific site or location. It provides a detailed representation of how data moves within a particular site, capturing the interactions between entities and processes unique to that site.

In summary, a data-flow diagram is a powerful tool for visualizing the flow of data in a system or process. While UML's activity diagram is commonly used in place of DFDs, site-oriented data-flow plans offer a specialized form of DFD that focuses on data flow within a specific site or location. These techniques aid in structured analysis, data modeling, and understanding the data dynamics within an information system.

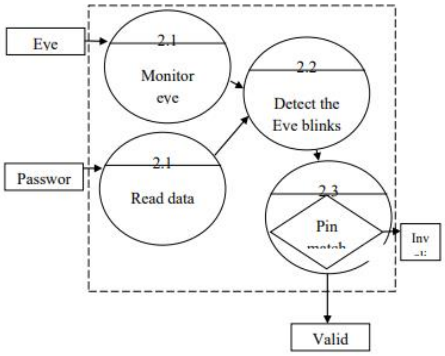
Level: 0 describes the overall process of the project. We are using users eye blinks as input. System will use the opencv haar cascade classifier to secure user account information from shoulder surfing attacks.



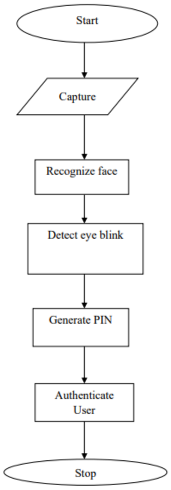
Level: 1 describes the first step of the project. We are passing user credentials as input. System will use the opencv haar cascade classifier to generate eye blink based password.



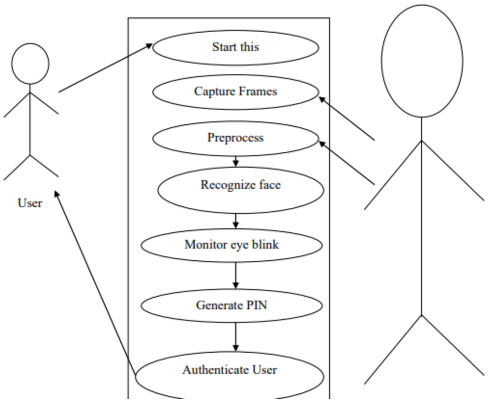
Level: 2 describes the final step of the project. We are passing user credentials from database and generated password as input. System will verify and authenticate the user is authorized or not.



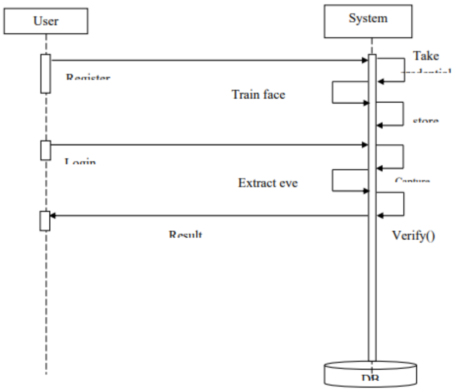
Flow chart



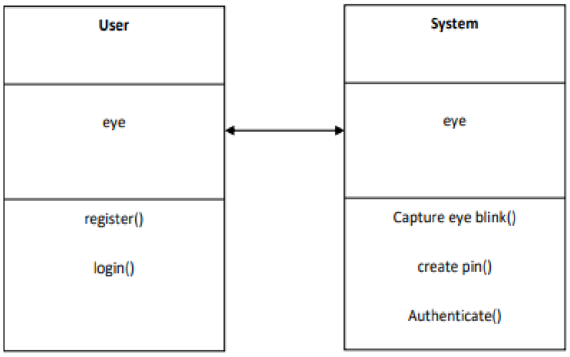
Use Case Diagram



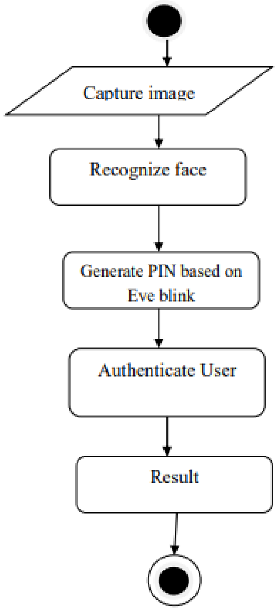
Sequence Diagram



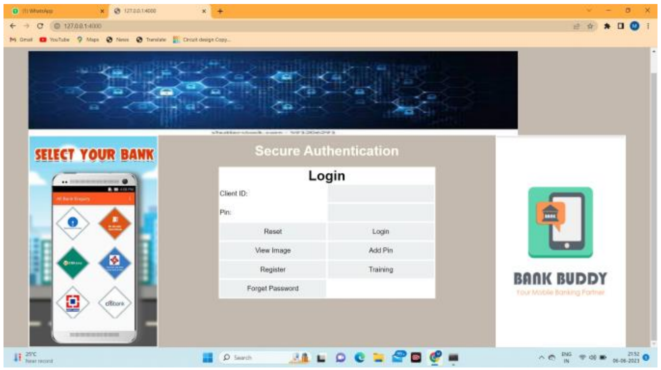
Class Diagram



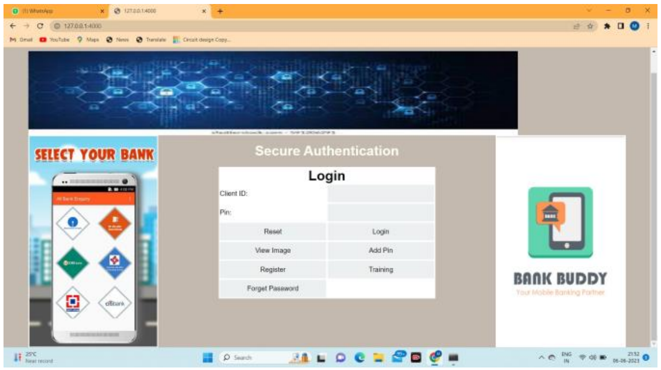
Activity Diagram



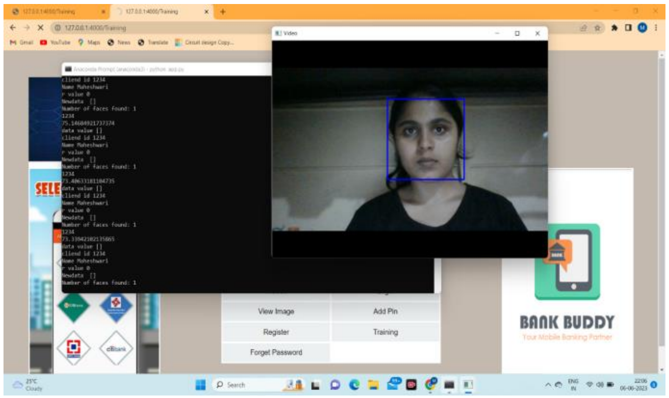
VII. RESULTS



Home page

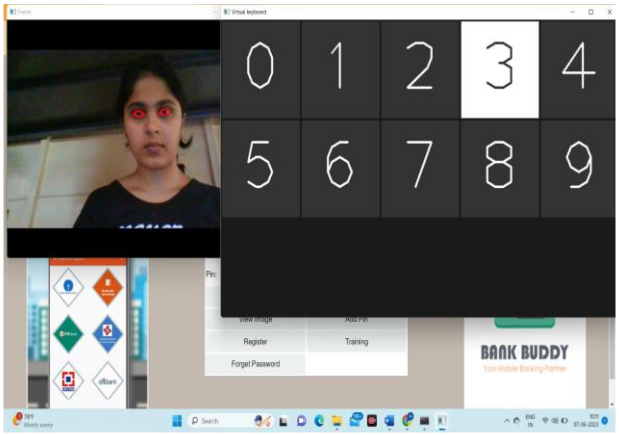


Register page

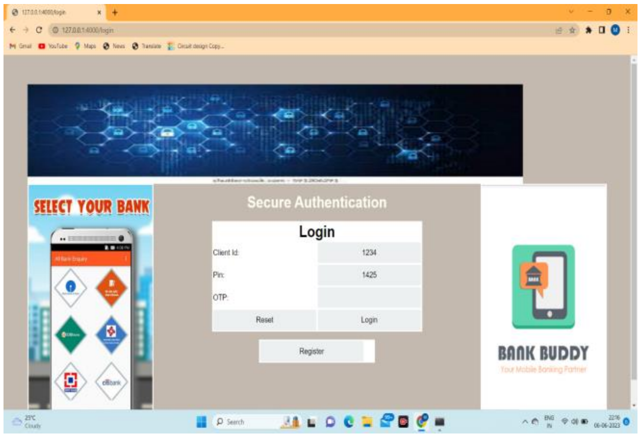


```
cliend id 1234
Name Maheshwari
r value 0
Newdata  []
Number of faces found: 1
1234
75.14684921737374
data value []
cliend id 1234
Name Maheshwari
r value 0
Newdata  []
Number of faces found: 1
1234
73.48633181184735
data value []
cliend id 1234
Name Maheshwari
r value 0
Newdata  []
Number of faces found: 1
1234
73.33942182135865
data value []
cliend id 1234
Name Maheshwari
r value 0
Newdata  []
Number of faces found: 1
```

viewImage page



Eye-blink page

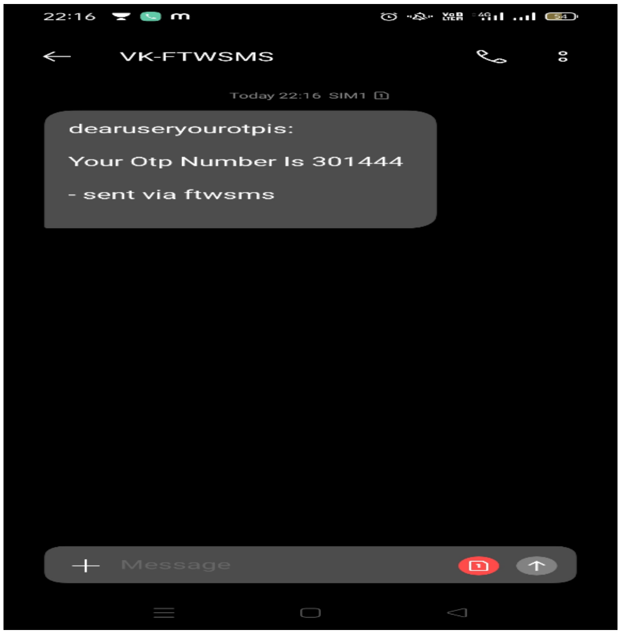


Secure Authentication

Login

Client Id:	1234
Pin:	1425
OTP:	

OTP-Generation

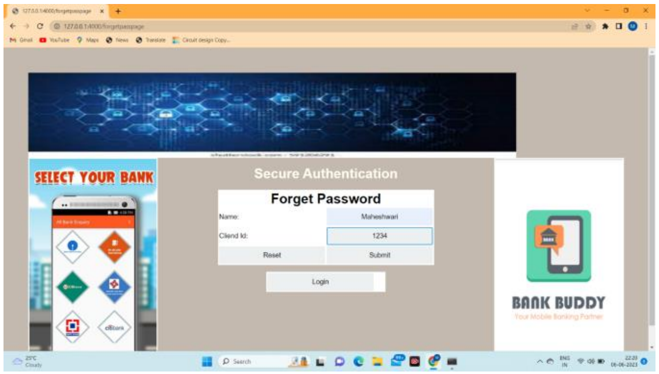


dearuseryourotpis:

Your Otp Number Is 301444

- sent via ftwsms

OTP



Secure Authentication

Forget Password

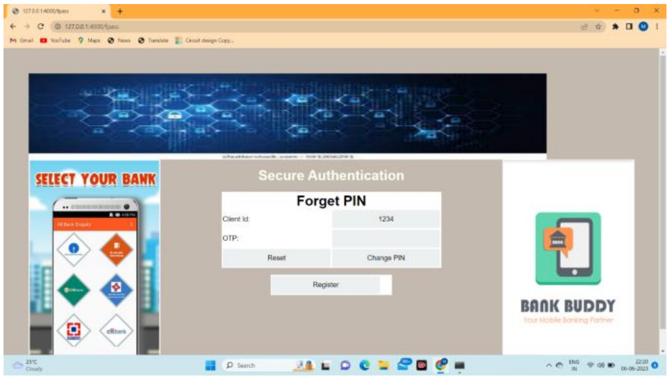
Name: Maheshwari

Clend Id: 1234

Reset Submit

Login

Forget-Password page



Secure Authentication

Forget PIN

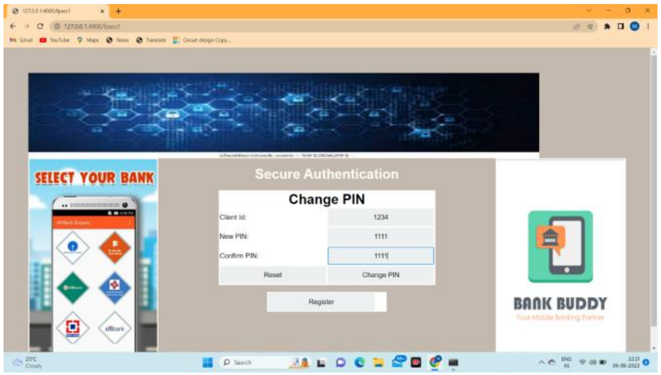
Client Id: 1234

OTP:

Reset Change PIN

Register

Forget-Pin page



Secure Authentication

Change PIN

Client Id: 1234

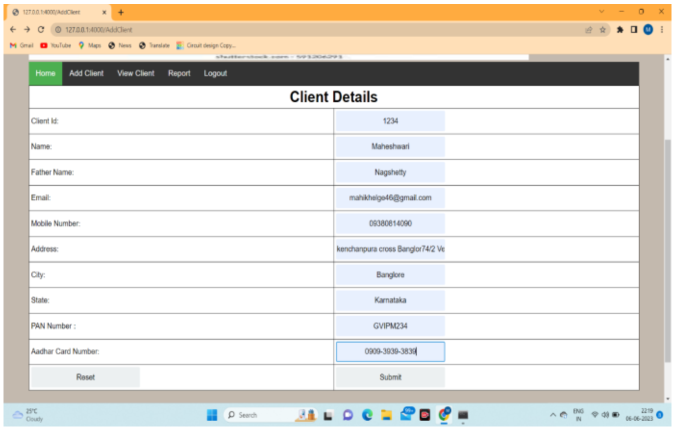
New PIN: 1111

Confirm PIN: 1111

Reset Change PIN

Register

Change-Pin page



Client Details

Client Id:	1234
Name:	Maheshwari
Father Name:	Nagshetty
Email:	mahikhelge46@gmail.com
Mobile Number:	09380814090
Address:	kenchanpura cross Banglor74/2 Ve
City:	Banglore
State:	Karnataka
PAN Number :	GVIPM234
Aadhar Card Number:	0909-3939-3839
Reset	Submit

VIII. CONCLUSION

A novel application has been developed that incorporates a web-camera based eye-tracking system for gaze-based PIN identification. The system has been successfully tested using a nine-digit keypad and can be extended to accommodate character and digit combination passwords. The eye blink ratio between digits is used as a distinguishing factor for PIN identification.It is important to note that the precision within the clusters of digits can be affected by the screen size, requiring calibration for each screen and keypad combination. Additionally, the stability of the user's gaze plays a role in the accuracy of the detected PINs, necessitating appropriate adjustments.The incorporation of this eye-tracking technology addresses common drawbacks associated with traditional password entry methods, such as the risk of forgetting passwords and potential leakage. It offers a highly secure alternative for authentication. The versatility of this technology makes it applicable to various sectors in the corporate world.Furthermore, the potential applications of this method can be expanded for use in high-end security systems by conducting further research and making improvements at an advanced level. One notable improvement is the system's compatibility with affordable and portable USB cameras, as opposed to expensive high-resolution color video CCD cameras. These USB cameras, such as Logitech models, offer higher real-time frame rates of up to 30 frames per second.The reliability of the system has been demonstrated through high accuracy results reported in previous sections. Experiments have shown that the system performs well even in extreme lighting conditions, such as when all other lights are turned off and only the computer monitor or a direct lamp light is available. The accuracy percentages obtained in these cases are comparable to those achieved under normal lighting conditions.In summary, the incorporation of web-camera based eye-tracking technology for gaze-based PIN identification offers a secure and convenient method for password entry. Its compatibility with affordable USB cameras, reliability in various lighting conditions, and high accuracy results make it a promising solution for enhancing security systems across different domains.

REFERENCES

[1] R. Revathy and R. Bama, “Advanced Safe PIN-Entry Against Human Shoulder-Surfing,” IOSR Journal of Computer Engineering, vol 17, issue 4, ver. II, pp. 9-15, July-Aug. 2015. (Available: http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue4/Version2/B017420915.pdf)

[2] J. Weaver, K. Mock and B. Hoanca, “Gaze-Based Password Authentication through Automatic Clustering of Gaze Points,” Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct. 2011. (DOI: 10.1109/ICSMC.2011.6084072)

[3] “ATM Fraud, ATM Black Box Attacks Spread Across Europe”, European ATM Security Team (E.A.S.T.), online, posted 11 April 2017. (Available: https://www.europeanatm-security.eu/tag/atmfraud/)

[4] K. Mowery, S. Meiklejohn and S. Savage, “Heat of the Moment: Characterizing the Efficacy of Thermal CameraBased Attacks,” WOOT ’11, pp. 1-8, August 2011. (Available:https://cseweb.ucsd.edu/~kmowery/papers/thermal.pdf)

[5] M. Mehrübeoglu, H. T. Bui and L. McLauchlan, “Real-time iris tracking with a smart camera,” Proc. SPIE 7871, 787104, 2011. (DOI:10.1117/12.872668)

[6] M. Mehrubeoglu, L. M. Pham, H. T. Le, M. Ramchander, and D. Ryu, “Real-time eye tracking using a smart camera,” Proc. 2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR ‘11), pp. 1-7, 2011. (DOI: 10.1109/AIPR.2011.6176373)

[7] M. Mehrubeoglu, E. Ortlieb, L. McLauchlan, L. M. Pham, “Capturing reading patterns through a real□time smart camera iris tracking system,” Proc. SPIE, vol. 8437, id. 843705, 2012. (DOI: 10.1117/12.922875)

[8] Smart Cameras for Embedded Machine Vision, (product information) National Instruments (Available: http://www.ni.com/pdf/products/us/cat_ni_1742.pdf