JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Multimedia Graphical Authentication

Dr. Madhu B, Raveena Hebbar, Rohith S Patil, Shubhada BN, Shubham Kumar Saras
Assistant Professor, Student, Student, Student, Student
Department of Computer Science and Engineering,
Dr. Ambedkar Institute of Technology,

Abstract : Today, everyone uses the internet as a common medium for communication. The risk to the multimedia data that we transfer from one end to the other end increases as internet usage increases. Passwords are one of the widely used methods for secured communication. Every kind of global communication uses a password as a means of authentication. The most well-known technique is to utilize a text-based password. The enhancement to the existing text based password is to use multi-level graphical password authentication provides an alternative to traditional text-based passwords, addressing their limitations. With graphical passwords, users can select images, patterns, or gestures as their authentication method. This approach enhances memorability as humans tend to remember visual cues better than complex alphanumeric passwords. It also improves security by increasing the search space and resistance to dictionary-based and brute-force attacks. Graphical passwords offer a user-friendly and inclusive experience, catering to individuals with difficulty remembering text-based passwords or visual impairments.

Keywords: Password, Image Photographical Authentication, Image Processing, Secret Key, Video Frames

I. Introduction

Regular passwords are susceptible to several sorts of attacks, to offer a more secure and relaxed authentication method, a photographic authentication is presented on this page. Here we provide user protection and authentication. This project includes parts, picture processing the usage of the selected click on vicinity and video processing the usage of click on durations, wherein your mixture of each will generate a password for the person to sign in. Popular methods include text-based secret words and picture-scrambled secret key confirmation. Although simple and secure, shoulder surfing attacks can still be successful with image passwords. Key logging software is used to increase security in person authentication and stop unauthorized users from seeing or changing the statistics of other users. The login secret phrase is a combination of Email Id, Password, photograph, and video click area, and the password is made up of a series of images and a video signature. Every password is individually encrypted and kept secret, even from developers.

II. LITERATURE REVIEW

Hybrid Textual-Graphical Authentication Scheme with Memorability, and Usability was suggested by Shah[1]. Alphanumeric and draw metric patterns is utilized to generate the passwords. The method creates its own threat model to check against different. The cross image-based authentication method is suggested to choose their password . The difficulty of the proposed method is to remember the password sequence. Our project is a user friendly application, where the passwords are more memorizable and it aims to provide various layers of image and video graphical password which in turn promotes the secured life to the user.

The EYEDi graphical authentication scheme, proposed by Takayuki Kawamura et al., aims to enhance the security of authentication systems by generating various distorted images for user authentication. The methodology involves the generation of distorted versions of original images using multiple image processing filters, with the appropriate filter strength estimated based on the user's authentication data. However, compared to image and video password authentication methods, EYEDi has certain drawbacks. It requires additional time for authentication due to image distortion and filter processing, which may be seen as a disadvantage compared to quicker authentication processes. Our method is quite simple and easy, not complex. The time taken is less and no extra time is needed for authentication to image distortion.

Web Based Password Authentication System in 2021 presents a novel approach to address the challenges of using a third party in password authentication. The authors propose a unique time-based password scheme that enhances security. However, the drawbacks of these approaches include the difficulty in remembering textual passwords with various combinations, the limited two-step authentication process consisting of a basic textual password and an image-based password. Moreover, the research process entails architectural complexity, and the authentication process itself can be time-consuming. In our project time consuming is less and it is more secured where multilevel authentication is provided to user.

Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure was suggested by Ashok Kumar Das ,Basudeb Bera ,Mohammad Wazid,Sajjad Shaukat Jamal and Youngho Park.They have offered some solutions to assist construct a more secured and functional user authentication method that provides security to the next generation of IoT infrastructure .The fuzzy extraction method for biometrics verification is implemented here for more security. In our project we have used graphical passwords ,which is significantly advantageous over biometric passwords as it rely on physiological or behavioral characteristics that users may find harder to recall or replicate accurately. On a variety of devices, graphical passwords can be utilized without specialized hardware or sensors. Contrarily, biometric passwords frequently rely on certain biometric sensors, like fingerprint scanners or facial recognition cameras, which might not be widely accessible or compatible with all devices.

"A Hybrid textual password authentication system with enhances security" paper is proposed to enhance security, many systems have employed a hybrid model of both textual and image authentication systems. A two-factor authentication mechanism is used . In order to use this, a user must first register by selecting a unique collection of 5 photos and entering his personal information (such as a username and password). At authentication time, once the user has provided his login and password, they will be shown with a series of photos and asked to choose one from each cycle. It is not secured and does not prevent any attacks. In our software where it can reduce multiple attacks and even video based authentication is provided.

The paper "Password Manager with Multi-Factor Authentication" by R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan, and Saleem Basha proposes a password manager that securely stores and encrypts passwords, incorporating multifactor authentication with physical security keys and graphical passwords. The system architecture consists of four modules: Master password, Vault Key, Multi-Factor Authentication, and Web server. The master password is hashed using PBKDF2 to ensure secured storage. However, PBKDF2 introduces computational overhead and slower authentication time, unlike our proposed project. Additionally, unlike the paper, our project does not involve hardware-based tokens. Graphical passwords are cost-effective, easy to remember, and do not require additional hardware.

Enhancement of Authentication System Using Vector (Graphical) Images by Karan Pandey, Amitesh Singh, Ashutosh Anand, Abhishek Kaushik and Shiv Narain Gupta narrates the usage of vector-based authentication system which is the best alternative for text password, With the help of Persuasive Cued Click Point (PCCP).This only involves image level authentication which might be susceptible attacks. Our project involves both image and video-level authentication which provides higher level of security comparatively to the one described in this paper. Compared to image password authentication, graphical video password authentication is more secured because it includes the element of time, which makes it more difficult for attackers to record and replicate the precise sequence of actions necessary for authentication. This increases the complexity of the password provided by the user and lowers the risk of unauthorized access.

The paper "Implementation of 3-Level Security System Using Image Grid Based Authentication System", the three-tiered security system is unquestionably a strategy that is time-consuming due where the user is required to navigate through all three tiers of protection and must refer to his email address in order to obtain the one-time password that is produced automatically, this system cannot be a good answer for general security the complexity that will be introduced by the passage of time. The password space is very small and requires lot of manual effort to operate it, whereas our paper is very easier to operate and less time consuming. More security is provided in our project and otp will be sent to mobile number which is less time consuming compared to email address.

The paper "Improved Arbitrary Password Authentication for Web Application Safety", focuses on improving graphical authentication for web applications. The authors emphasize the importance of unique and secure passwords to protect against unauthorized access. Traditional text-based passwords can be challenging to remember, which is why graphical passwords have become popular. Users log in to the system using photos they choose from a grid in this method. The study examines several recognition, recall, and cued recall authentication methods for graphical passwords. The suggested remedy seeks to address the shortcomings and weaknesses of current systems, including dictionary attacks, brute force assaults, guessing attacks, and shoulder surfing. The study proposes boosting the security and usability of passwords by using graphical authentication. The authors perform a study on graphical password authentication, offering analysis and a theory for user authentication and system or website login. The study seeks to increase overall security and address the drawbacks of conventional alphanumeric passwords.

III. METHODOLOGY

Multilevel authentication systems use the adaptation of text based passwords in the initial phase. At the next level, the algorithm wasverified and recognized using the pixel-matching technique of an image.
The following level corresponds to the quantity of frames in the video input. The user will receive a final acceptance based on the OTP. Users in this project will have a choice between registering or logging in when trying to view the Homepage. The first steps in the procedure are as follows:

Phase of Registration

1. Information like first and last names, email addresses, passwords, etc. will be entered on the registration page.
2. After clicking the next button, a graphical password security page with an image-based password will be shown.
At some stages, the opportunity to select the image is shown.
3. A website that asks for a password selection based on the video frames' visual sequence.

User Login

When attempting to access the Homepage in this article, users will have two options: register or log in.
1.In such case, the login option is chosen if the user has already registered.The correct username and password are then typed. The user can log in successfully if their text-based password and username are both accurate.
2. Following the appearance of the Image Base Password screen, the user must select the Image checkpoints password. The nextpage was redirected once the image pixels were matched.
3. The screen for the video base password will then appear, a user must choose the image frame number of videos based on passwords. The order of the frame numbers should be matched to move on to the next level.
4. If the user receives a successful OTP, the banking home page will be displayed.

A new technique for establishing the password to increase memorability was the draw metric process. The security of the suggested system against keystroke/mouse logger attacks, dictionary attacks, shoulder surfing, random guessing, phishing or form-taking, and multiple recording attacks has been tested. Several trends in the items used and the accompanying authentication durations were reported as we also examined the usability and memorability of the password. The results and research demonstrate how effective the proposed approach is. Due to the wide range of novel solutions it brings, we believe the offered method offers a number of opportunities for innovation in security operations.

The Client must first visit the website internet page in order to access the records. Additionally, the customer must sign in byselecting frames in the video that are consistent with their choice for signing into page and picking prompt focuses during such images. They must select the same prompt options that they decided upon earlier in the enrollment process on the login page.The consumer must fill out the join page with their full name, username, picture signal snap variables, and video prompted spans, which ar e stored in the insights base while the individual registers.

If the customer attempts to log in again, they must select the identical snap factors; if they do so, the login will be successful. If the sign centers don't match the brief centers already saved during enrollment, a pop-up message stating that the data is "invalid" may appear.

The person then longs to try signing in again with the proper prompt variables at that moment. In the case that the login is successful, the user receives the privilege of access to the official reports to down stack or transfer for more opportunities.

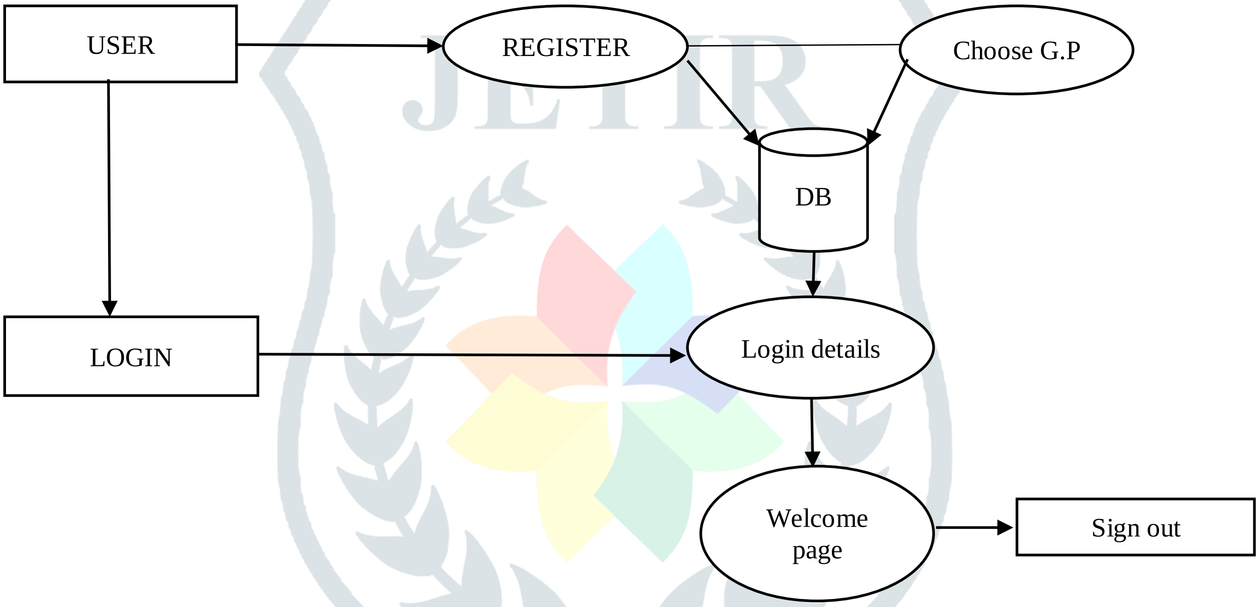


Fig.1: Block Diagram of System Design

The image's sign focal points should be an image focused on the most important factor. The video selection should be appropriate such that the choice of stretch is obvious and done superbly or extraordinarily easy to hack. Here, the combination of sign markings from video and image gives an encoded secret phrase for the client to login. The client no longer receives a verified login if all signers determine that either the photo or the video is incorrect.

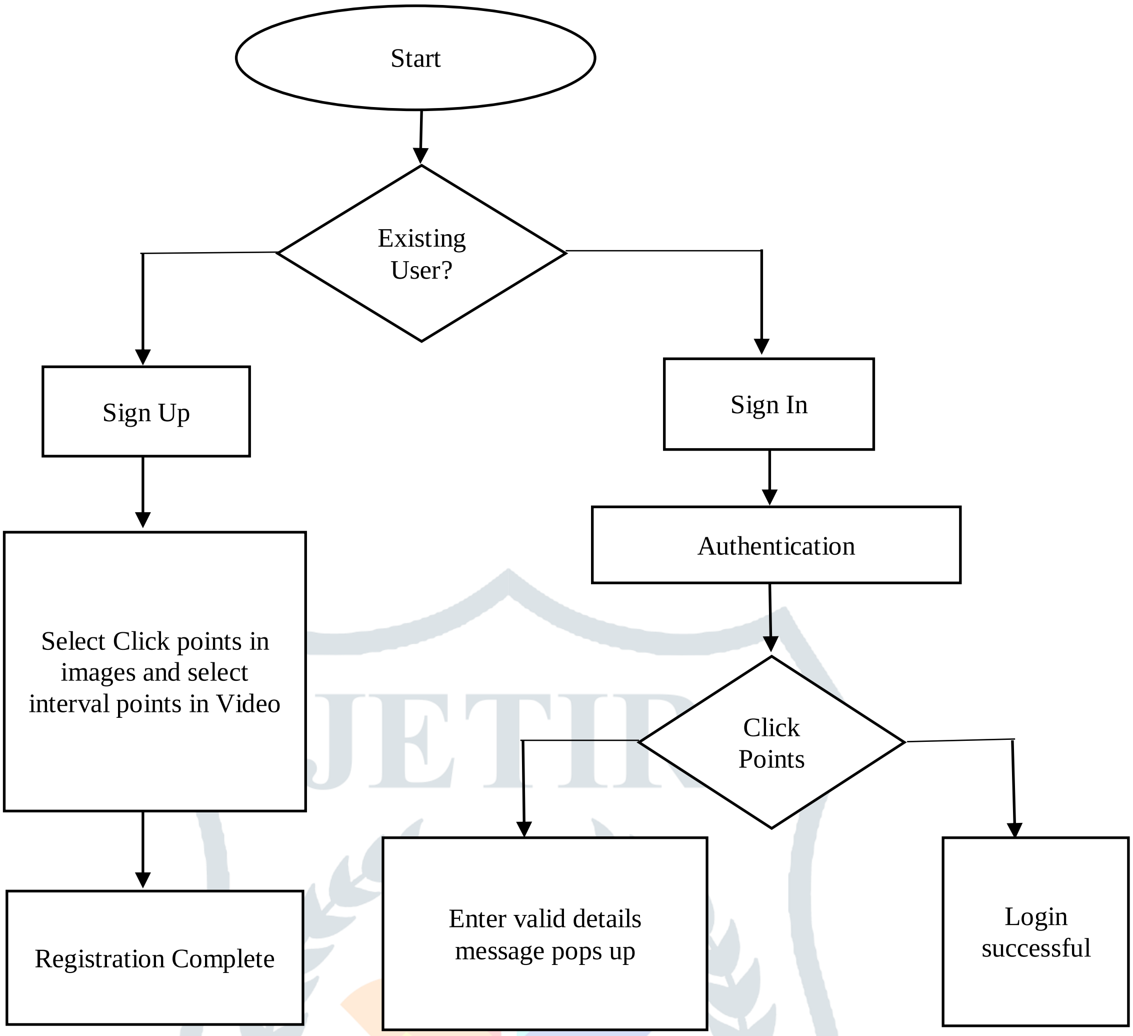
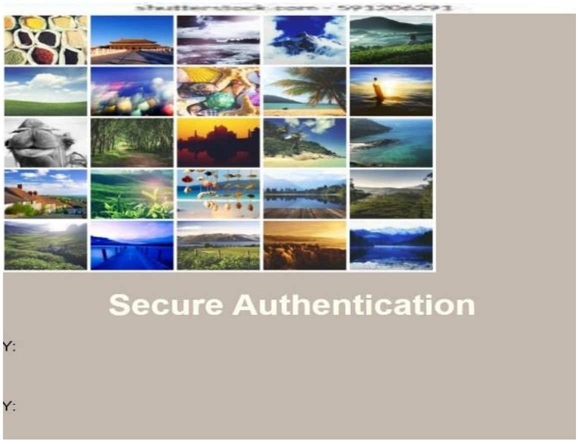

Start
Existing User?
Sign Up
Sign In
Select Click points in images and select interval points in Video
Authentication
Click Points
Registration Complete
Enter valid details message pops up
Login successful

Fig.2: System Flow Chart

Figure 2 represents the flowchart of the user registration and follow the steps to login where he has to select the image followed by frame numbers of a video if the user does not exist . If already a user, then should match the correct password to login.

IV. RESULTS AND DISCUSSIONS

Our research effort has proven the value of using picture and video-based techniques for user authentication by implementing Graphical User Authentication. The probability of dictionary assaults, brute force attacks, guessing attacks, and shoulder surfing attacks is considerably reduced by the combination of textual passwords, click points, and shuffle methods. Compared to typical text passwords, graphic passwords are easier to remember, making them a more efficient and safe form of authentication. Our investigation' findings suggest that using graphical password systems is a smart way to improve user authentication and reduce security flaws. Overall, our project produced results that are 80% accurate and efficient.

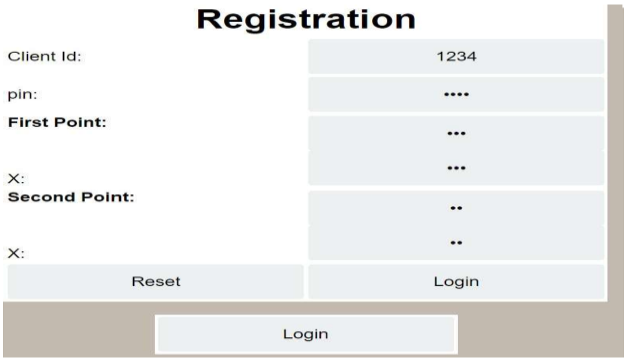

Secure Authentication

Y:

Y:

Fig.3: Image-Level Password Selection

Image level password selection is indicated in Figure 3.Our method introduces a novel approach for secure authentication through the utilization of a collection of images, enabling users to select a password at the image level. This authentication method enhances security and usability by offering an alternative to traditional text-based passwords.



Registration

Client Id: 1234

pin: ••••

First Point:

X: •••

•••

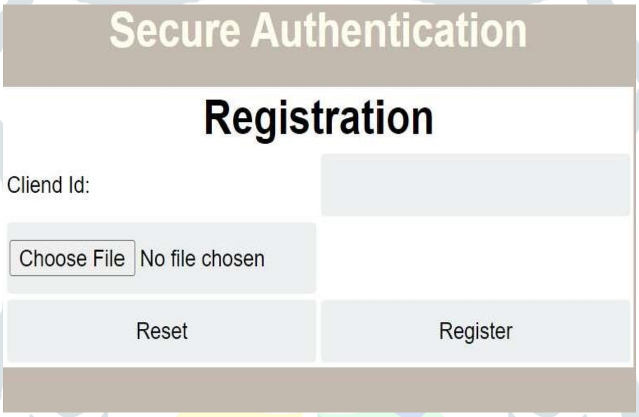
Second Point:

X: ••

••

Fig.4: Image pixel values

The Fig.4 illustrates the procedure of configuring a password by providing pixel values based on the client ID. Users are required to input the pixel values corresponding to their chosen password configuration. Additionally, users are provided with the option to reset their password or proceed with login using the provided pixel values.



Secure Authentication

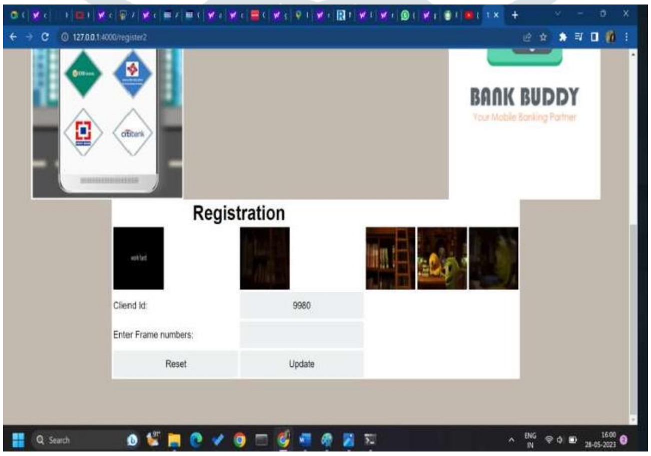
Registration

Cliend Id:

Choose File No file chosen

Fig. 5: Updating of Video

Figure 5 indicates the authentication process at the video level, where users input their ID and select a video for configuring a video-based password. Upon selecting the video, users can click on the 'Register' button to proceed with the authentication process."



127.0.0.1:4000/register2

BANK BUDDY

Your Mobile Banking Partner

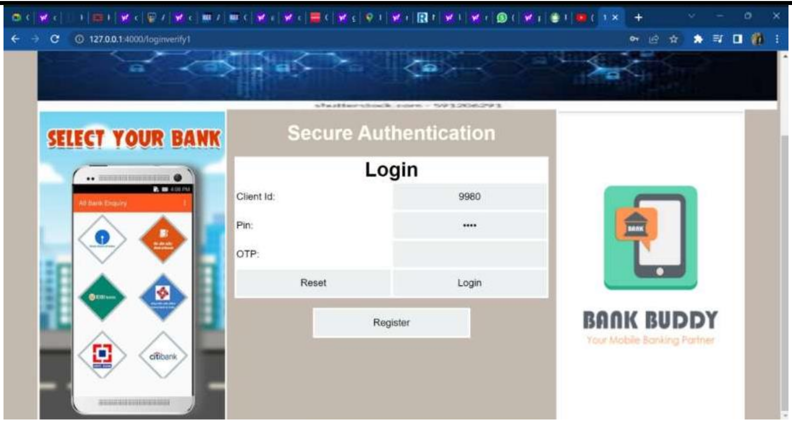
Registration

Cliend Id: 9980

Enter Frame numbers:

Fig.6: Video converted to frames of images

The procedure of video presents the video frames where video is converted into image frames user must select any number of the frame numbers and give it as a password.


127.0.0.1:4000/loginverify1

Secure Authentication

Login

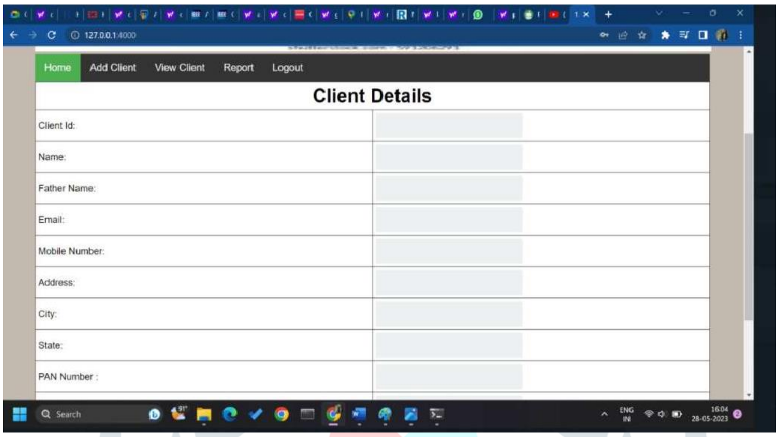
Client Id: 9980

Pin: ••••

OTP:

Fig.7: OTP level authentication

Final authentication level is given in Figure 7 as shown above .The OTP will be sent to the registered mobile number.


127.0.0.1:4000

Client Details

Client Id:

Name:

Father Name:

Email:

Mobile Number:

Address:

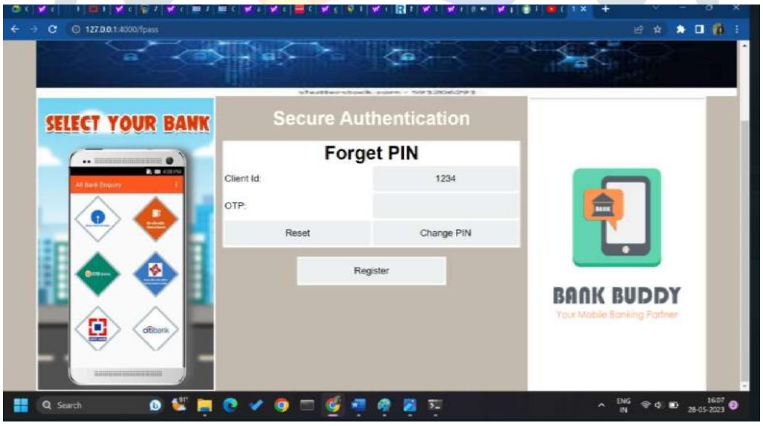
City:

State:

PAN Number :

Fig.8: After logging in, the home page

Figure 8 indicates the home page of the bank that is provided by the correct password and OTP by the user. The user now can login to hisactual banking website to continue with the transaction.


127.0.0.1:4000/fpass

Secure Authentication

Forget PIN

Client Id: 1234

OTP:

Fig.9: Forgot password page

Figure 9. Indicates forgot pin page, If a user forgets their password, they can replace it by entering the OTP that was supplied to their cell phone. As seen in Table 1, our technique is contrasted with the other ways. It is evident that our approach is superior to others.

Author	Year	Authentication Type	Technique	Limitations	Time
Shah[1]	2021	Draw Metric	Pattern, OTP	Operate Two Modes and Remembering Pattern	40.16s
Abhijit[2]	2021	Web Based	Pattern, Key	Platform Dependent	Not Mentioned
Ours	2023	Pixel Matching Video Frame	Text, Image, Video, OTP	NA	Less than a minute

Table 1: State of art Comparison

Table 1 depicts the comparison of state of art and our method. Shah[1] has introduced graphical based authentication with image pattern and OTP. The method operates in two modes easy and complex. The limitation of such a method is to switch over two methods. Abhijit[2] also given an algorithm for new web based authentication system. The main drawback of the method is dependency of platform. Our method uses simple pixel matching and frame ordering with video authentication method. The method is platform independent and the complete authentication process will take 30s to complete. So our method proves to be good with reference to the reference methods.

V. CONCLUSION

The world is rapidly becoming digital as a result of growing technological breakthroughs takes place through online. The customer would like to do online transaction for everything like bill payment, reservations for events, banking transactions etc. Other online activities include communication through email and messaging applications, document storage, and more. Everything moving online has increased the possibility of cybercrimes and privacy violations. The data should be is kept safe on both online and offline platforms. The standard way of authentication to access our accounts is passwords. The normal passwords can be easily traced using trial and error methods. So the necessity of advanced password protection system for our day to day transactions. So the proposed method come up with the advanced authentication system using image and video. The algorithm makes it difficult for the intruders to approximate about the password and the ongoing transactions. The experimental results depict that only text passwords are not sufficient for the banking transactions we need an advanced algorithm to protect our passwords. We can reduce assaults such as dictionary attacks, brute force attacks, guessing attacks, and shoulder surfing attacks by using a graphical password system.

In the future, there are several potential enhancements that can be implemented to further improve graphical password authentication. One area of focus is the integration of biometric authentication, such as fingerprint or facial recognition, to provide an additional layer of security and enhance user verification. Advanced gesture recognition algorithms can be developed to accurately analyze and authenticate complex gestures, improving the overall security and usability of graphical passwords. Context-aware authentication techniques can be explored to adapt the graphical password requirements based on factors like user location or device information, adding an extra layer of adaptive security. Additionally, multi-modal authentication approaches, combining graphical passwords with other factors like voice recognition or behavioral biometrics, can be investigated to create a more robust and reliable authentication system. Continuous authentication mechanisms can be implemented to monitor user behavior throughout a session and detect any suspicious activities or unauthorized access attempts. Furthermore, leveraging machine learning and AI algorithms can aid in detecting and mitigating potential attacks by analyzing user behavior patterns and identifying anomalies. Usability enhancements should also be considered to ensure a seamless and intuitive user experience. Finally, standardization efforts and industry collaboration can promote interoperability and the widespread adoption of graphical password authentication.

VI. REFERENCES

[1] Shah Zaman Nizamani, Syed Raheel Hassan, Riaz Ahmed Shaikh, Ehab Atif Abozinadah and Rashid Mahmood,"A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security, Memorability and Usability".Vol. 9 , Pages 51294-51312,2021.DOI:10.1109/ACCESS.2021.3069164

[2] Abhijith S, Soja Sam, Sreelekshmi K U, T T Samjeevan, Sneha Mathew "Web based Graphical Password Authentication System" IJERT, Volume 09 ,ISSN: 2278-0181, 2021. DOI: 10.17577/IJERTCONV91S07007

[3] Ashok,Babudeb Bera,Mohammed, Sajjid, "On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure" IEEE, Volume 9, 2021, DOI: 10.1109/ACCESS.2021.3079312

[4] Pathik Nandi, Dr. Preeti Savant "Graphical Password Authentication System" International Journal for Research in Applied Science and Engineering Technology, ISSN: 2321-9653, 2022, DOI Link: https://doi.org/10.22214/ijraset.2022.41621

[5] T. Y.Yang, P., Shamala, M., Chinniah, and C. F. M., Foozy. "Graphical Password Authentication for Child Personal Storage Application." In Journal of Physics: Conference Series, Volume. 1793, February, 2021, DOI 10.1088/1742-6596/1793/1/012065

[6] G. K., Jiya, I. O., Oyefolahan, and J. O., Ojeniyi, "Recognition Based Graphical Password Algorithms: A Survey",2nd International Conference on Cyberspace, IEEE,2021, DOI: 10.1109/CYBERNIGERIA51635.2021.9428801

[7] Z. A., Abdalkareem, F. A., Akif, Abdulatif,, A., Amiza, AND P., Ehkan, "Graphical password based mouse behavior technique". In Journal of Physics: Conference Series, Vol., IOP Publishing, February, 2021, DOI 10.1088/1742-6596/1755/1/012021

[8] Ajmeera Kiran, Ben Sujitha B, P.Vijayakarthik, Manduri Vamsi Krishna, Suragouni Nikitha "Implementation of 3-Level Security System Using Image Grid Based Authentication System", 2023 International Conference on Computer Communication and Informatics (ICCCI), Jan. 23 – 25, 2023, Coimbatore, DOI: 10.1109/ICCCI56745.2023.10128606

[9] "Password Manager with Multi-Factor Authentication" by R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan, and Saleem Basha,2023,DOI:10.1109/ICNWC57852.2023.10127424

[10] "Improved Arbitrary Graphical Password Authentication for Web Application Safety", Naga Sai Sindhu Chaluvadi , Lakshmi Chitteti, Lasya Challa, Srithar S,2023, DOI: 10.1109/ICSSIT55814.2023.10060964