Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing Access: A Combined Approach of Cued Click Points and Text Passwords for Authentication

Vaishnavi Palkonda[1], Viyyapu Lokeshwari Vinya[2], Niveditha Kolluri[2], Sahithi Godavarthi[2], Ravula Arun Kumar[2], Radha Mothukuri[2]

[1]Student, Department of Computer Science, Vardhaman College of Engineering, India, vaishnavipalkonda@gmail.com
[2]Assistant Professor, Department of Computer Science, Vardhaman College of Engineering, India

Authentication is one of the most important security primitives. Alphabetic password authentication is the most used type of authentication. It has been shown that this method has several shortcomings and is susceptible to several attacks, such as dictionary, brute force, and shoulder surfing attacks. The project follows a combined approach using graphic passwords in order to get over the limitations of alphanumeric passwords. This is because visuals are easier for people to recall than text. Before developing a new graphical password system, this essay seeks to highlight the usability features of the existing graphical Pass face system. It uses both text and graphic passwords to strengthen the desktop authentication process. These days, computers play a significant role in everyone's lives. This study introduces a novel multi-factor authentication (MFA) framework that combines traditional text passwords with advanced visual recognition techniques. By integrating text passwords, image selections, and point selections, our approach offers enhanced security while maintaining user-friendliness. This MFA model aims to address current limitations of single-factor authentication systems and mitigate risks associated with modern cyber threats.

Keywords: Authentication, Vulnerable, Brute Force, Dictionary Attack, Memorability, Security Considerations.

1. Introduction

The use of password authentication for authentication is dwindling. Users must input the user's username and password in order to authenticate them. Most apps allow the use of knowledge-based authentication, which includes graphical and alphabetic passwords. Because password systems are not memorable and are not secure, they frequently handle requirements that conflict. First, passwords ought to be sensible and easy to remember. It needs to be secure as the second requirement. In the fast-paced world of today, where users have multiple accountsand networks. Some sort of basic authentication framework must be offered[1].To

address various security concerns, password schemes have been criticized for being touted as a potential replacement for text-based passwords, particularly those because pictures are easier for people to recall than words. Pictures are usually easier to remember or more commonly recognized than words, especially pictures, which are even easier to recall than random images. Despite the fact that the current Pass face strategy includes a wide range of characteristics that make things easier to use or recall, as well as easier to identify and comprehend, there are various drawbacks to this method.

Setting a password with the mouse makes it simpler for an attacker employing a shoulder surfer to view the password. Furthermore, based on an additional study, customers typically select people who are similar to them, making it possible for attackers to figure out the algorithm. The objective of this work is to reduce the attack risk associated with shoulder surfing in order to make the Pass face algorithm safer. Therefore, in order to overcome the drawbacks of alphanumeric passwords, the project recommend using visual passwords instead.An attempt is made to use the human memory for visual information by means of graphic password systems, a sort of knowledge-based authentication.

The objective of this work is to reduce the attack risk associated with shoulder surfing in order to make the Pass face algorithm safer.Therefore, in order to overcome the drawbacks of alphanumeric passwords, the project recommend using visual passwords instead. An attempt is made to use the human memory for visual information by means of graphic password systems, a sort of knowledge-based authentication. These kinds of technologies allow users to locate and target pre-selected areas in one or more photographs. To help with recollection, the visuals serve as memory cues. Using pictures in place of conventional alphanumeric characters, graphic password authentication confirms a user's identification. Users can respond to photos shown in a specific order, choose images in a specific order, or draw graphics on a grid as examples of how they interact with images. The purpose of this technique is to improve security and user experience by taking advantage of the fact that images are easier for the human brain to remember than text-based passwords. Different approaches, such as recognition-based authentication, recall-based authentication, and cued recall, are available in graphical password authentication systems, and each has its own merits in terms of security and usability. These systems are intended to be easier to use, offer better security than conventional password schemes, and increase the difficulty of attacks like dictionary attacks and shoulder surfing.

Traditional passwords replaced with graphical images via an authentication technique called a graphic password authentication system. This is because people find it easier to remember pictures than words. Various graphical password schemes employ distinct strategies to lessen the impact of known attacks [1]. It is regarded as best practice to prioritize improved security over usability by include security measures in authentication. It can be challenging to strike a balance between security and usability, though. There is a chance that a certain graphical password method is more user-friendly but less secure, or more secure but less user-friendly[2].Our goal is to present a compelling case for adopting the proposed MFA system, The project's aim is to anticipate that this work will contribute valuable insights to both academia and industry stakeholders seeking innovative ways to improve account security.

One method for computer security authentication is the use of a graphic password. These days,

protecting user or customer data through digital/computer security is crucial to computer science. One issue that exists is shoulder surfing, which allows a hacker to obtain a password by either directly seeing the user or by recording the authentication process. There are a number of methods for achieving this authentication, the most popular and straightforward being the graphic password method. Thus, our project propose a novel method to tackle this issue.

The prevalence of cyberattacks in today's digital environment has made online account security more crucial. Text passwords alone or single-factor authentication (SFA) have flaws that make users vulnerable to different kinds of attacks. Multi-factor authentication (MFA)[3], which combines two or more independent verification processes, has emerged as a more reliable way to address these vulnerabilities. In order to improve security without sacrificing usability, our suggested MFA system expands on current SFA techniques and makes use of cutting-edge technology like computer vision and machine learning algorithms.

2. RELATEDWORK

The world is rapidly turning digital due to rapid technological breakthroughs, with everything taking place online. You like to make payments online for anything from bills to purchasing tickets to tipping the person seated across from you. Not only do transactions take place online, but so do all other activities including email and messaging app communication, document storage in digital lockers, etc. Everything is going online, which raises the possibility of privacy violations and cybercrimes. Passwords are essential for protecting your data on both offline and online platforms. The standard way of authentication that grants us, access to our accounts is passwords. Users can secure their accounts with a variety of authentication methods. Authentication types: [1]

Smart cards, bankcards, and key cards are examples of token-based authentication.

Text-based and picture-based authentication are examples of knowledge-based authentication.

Facial recognition, iris scanning, and fingerprint authentication are examples of biometric authentication.

Recall-based authentication requires users to verify their identity by duplicating an item they chose or made during the registration process. This method is in contrast to cued recall, in which users click on specified points inside photos, and recognition-based authentication, in which users recognize pre-selected images. Recall-based authentication requires users to authenticate by precisely replicating a certain action or choice they made during the registration process. For example, in the Passpoint system, users click on points within an image to construct a password. They then have to choose these points in the correct order during authentication. This approach improves security by making people remember certain activities or choices instead of just identifying pictures. Recall-based authentication is more secure and resistant to attacks such as dictionary attacks and shoulder surfing, but it can take longer to register and log in since precise replication of user-created items is required. Furthermore, compared to conventional text-based passwords, the usage of photos in recall-based authentication could need additional storage space. Recall-based authentication, in spite of these drawbacks, offers a convenient and safe substitute for conventional password systems,

increasing overall system security and providing greater resilience to frequent security attacks.

Alphabetic passwords in the traditional username-password authentication scheme are either difficult to remember or simple to guess. In addition, people usually use the same password for all of their accounts because it is difficult to remember many ones. Other authentication methods, such biometrics and graphical passwords, are used to address these problems with the traditional username-password authentication scheme. Using a graphical user interface (GUI), the user of a graphical password authentication system[4] must select from a list of images that are shown to them in a pre-set order.[5]

Recognition-based Authentication: After registering, a user must correctly recognize the image from a series of photos [6]. One graphical password technique based on facial recognition is Pass faces. Users can choose from a wide selection of photos when creating a password. Users must choose the pre-selected image from among the dozens that are displayed to them in order to log in [7].

Recall-based authentication requires the user to duplicate an item they chose or generated during the registration process [2]. For instance, the Passpoint scheme [7] allows the user to generate a password by clicking any point in an image, and it calculates a tolerance around each pixel. The user must choose the points within the tolerance in the right order during authentication in order to log in. Users for can draw passwords as long as they choose. In order to verify their identity, users must reapply their password. The broad theoretical space provided by this strategy is similar to that of text passwords. It has been demonstrated that users generate symmetric and centered passwords with this approach, which may make them easier for attackers to guess.

Identification of previously encountered information from a group of possibilities is the process of recognition-based retrieval. This method requires people to identify the proper information from a set of cues or choices. Generally speaking, recognition exams offer more cues than cued recall tests, which facilitates people's ability to recall the right material. In recognition-based authentication, users verify their identities by identifying pre-selected images or cues. This approach requires users to identify and choose the appropriate image or cue from a selection of images that they are shown during registration. In contrast, recall-based authentication requires users to replicate something they chose or made while registering. Passfaces is one example of a recognition-based authentication technique in which users register by choosing a particular face from a wide collection of photos. Users must accurately recognize the pre-selected face from a set of shown photographs in order to log in. This technique increases the memorability of passwords by taking use of the human brain's propensity to recall visuals over alphanumeric characters. However, there can be drawbacks to recognition-based authentication, like the requirement for enough picture storage capacity and the possibility of vulnerability to shoulder surfing attacks. Despite these limitations, recognition based authentication is a useful substitute for conventional text-based password schemes due to its enhanced security and user-friendliness, which strikes a balance between usability and security in authentication systems.

Cued Recall: An alternative to the PassPoints method is Cued Click Points (CCP)[8]. Unlike PassPoints, where users click five points on a single image, with CCP users click one point on each image. It provides cued-recall and notifies users immediately in case they type their click-

point incorrectly.[9]A technique known as ”cued recall-based authentication” involves giving users specific cues or suggestions to help them remember their password during the authentication procedure. Cued recall provides users with a framework of suggestions, context, or cues to help them accurately reproduce their password, in contrast to pure memory-based authentication where users must reproduce their password without any cues. This strategy seeks to improve authentication systems' accuracy and usability by giving consumers more assistance in remembering their passwords.By offering users a formal framework to assist with password retrieval, cued recall-based authentication systems achieve a balance between security and usability that is comparable to pure recall approaches. By utilizing cognitive cues and human memory processes, these systems enable precise password replication and provide an efficient and user-friendly authentication process. Cues or clues are incorporated into cued recall-based authentication techniques to help users reliably recall and reproduce their passwords during the authentication process, hence improving password security and memorability overall.

Hybrid Graphical Password Scheme: It combines the features of a passcode scheme and a recall method. In the registration phase, users choose a story-like series of photos from an image pool in a specific order. Subsequently, the user selects one or many photos and uses a sequence of clicks on the chosen images to create a hidden picture. Users have to replicate their secret photo in the right spot and choose the previously chosen images in the right order during the authentication process. [10]Hybrid retrieval methods combine aspects of recall-based and recognition based strategies. These methods may involve a combination of free recall, cued recall, and recognition techniques to optimize memory retrieval processes. Hybrid models aim to leverage the strengths of both recall and recognition strategies to enhance memory performance. The strengths of each methodology are combined in hybrid-based authentication systems to improve security and usability of the authentication process. The sources describe a safe hybrid authentication system that combines Press Touch Code and Passpoint techniques together in a smooth manner. With Passpoints, users have to pick certain locations within photos, and with Press Touch Code, they must press on a touch-sensitive surface to enter a code. The hybrid scheme provides a multi-layered approach to authentication by merging these two techniques, making the system more secure overall and making potential attackers' job more difficult.

PassPoints: During registration, users mark particular spots or regions on an image. They have to duplicate the selected point sequence in order to authenticate. [7]

Moreover, an initial user survey that produced encouraging findings indicated that the project prioritizes usability factors including speed, accuracy, and error reduction. Users cited the simplicity of choosing and remembering just one point per image as one reason for favoring CCP over more conventional techniques like PassPoints. An easy-to-use authentication process is enhanced by the system's design, which prompts users to recall the location of the appropriate point upon viewing each image. The project highlights that, in terms of security, CCP provides better protection than other techniques such as PassPoints since it makes it more difficult for attackers to carry out their attacks because it requires a greater number of photos for authentication. The project's objective of offering a reliable and secure graphical password authentication method is in line with this increased security feature. With a heavy emphasis on usability, security, and user preference, the project's overall scope encompasses the design,

implementation, and assessment of a graphical password authentication system employing Cued Click Points. The project seeks to provide a safe and efficient substitute for conventional text-based password systems using novel cued-recall algorithms and user-friendly design components.

3. PROPOSED METHOD

The world is rapidly turning digital due to rapid technological breakthroughs, with everything taking place online. You like to make payments online for anything from bills to purchasing tickets to tipping the person seated across from you. Not only do transactions take place online, but so do all other activities including email and messaging app communication, document storage in digital lockers, etc. Everything is going online, which raises the possibility of privacy violations and cybercrimes. Passwords are essential for protecting your data on both offline and online platforms. The standard way of authentication that grants us access to our accounts is passwords. Users can secure their accounts with a variety of authentication methods. A thorough analysis of the various graphical password techniques already in use is conducted as part of the literature review for graphical password authentication in order to determine their advantages, drawbacks, and potential applications. Scholars have classified graphical passwords into two categories: recall-based and recognition-based, each with its own benefits and drawbacks. While recollection-based schemes require users to recall a series of actions or click points within images, recognition-based schemes rely on users recognizing previously selected images.

In an era where cybersecurity threats are ever evolving, the need for robust and user-friendly authentication systems has become paramount. The project at hand aims to address this challenge by proposing a novel three-step authentication system that combines traditional text passwords with graphical elements. By integrating both types of passwords, this system seeks to enhance security while ensuring a seamless user experience.

The technology encourages users to choose intricate and unpredictable click points inside photos in an effort to provide a more secure authentication technique. By making it more difficult for hackers to guess passwords, this method improves system security as a whole. The project's enhanced authentication process with graphical passwords and cued click points is made possible by a number of important techniques that improve security. To begin with, the system pushes users to choose intricate and unpredictable click points inside photos, which makes it harder for password guessers or hackers to obtain credentials. By using this method, the system becomes far less susceptible to popular assaults such as dictionary, brute force, shoulder surfing, and guessing. Through the use of graphical components and cued click locations, the system enhances user experience by offering a simple authentication process while also bolstering security. Furthermore, by precisely validating the drawn images, the application of deep learning models for image classification offers an extra degree of security. Thanks to this cutting-edge technology, the authentication procedure is reliable and impervious to attempts by unauthorized parties to get access. Furthermore, by broadcasting only the color pixels of drawing images rather than the complete image, the suggested method of "selected pixels (SP)" improves efficiency and minimizes data transmission requirements while optimizing network performance.

For a very long time, the most popular method of authentication was passwords. Traditionally, they use characters that are alphanumeric. Nevertheless, there are a number of security issues with text-based passwords, including the difficulty of remembering intricate letter sequences and their susceptibility to brute force assaults.

Images, patterns, or a mix of the two is used as authentication in graphical passwords. Users choose or create images, draw patterns, or carry out other graphical tasks to authenticate themselves instead of using alphanumeric text. The following is the recommended procedure.[11]

A graphical password authentication system called the Persuasive Cued Click-Point (PCCP) algorithm was created to increase the security and usability of graphical passwords. It makes use of the notion that users frequently click on particular areas or spots in an image to verify their identity. The PCCP algorithm encourages users to select a sequence of click-points that are meaningful to them, making it harder for attackers to guess the correct sequence.

An alternate method to PassPoints is Cued Click Points (CCP)[8]. CCP enables users to click one point on each image, in contrast to PassPoints, which demand five clicks on one picture. Users are notified instantly in the event that they input their click-point inaccurately, and cued-recall is provided. In PassPoints, a password consists of five click-points. The user has the option to designate any pixel in the image as the password click point. To log in, they have to click in the correct order and inside the tolerance square of the first click sites as defined by the system.

All things considered, the project's emphasis on fusing the advantages of graphical passwords with the strengths of regular passwords produces a very secure authentication system that beats conventional techniques in terms of security metrics. This project not only offers a flexible platform that can be seamlessly integrated into various digital ecosystems, but it also enhances security through the integration of deep learning-based Arabic digit recognition and innovative transmission methods. As such, it is a promising solution for secure and user-friendly authentication processes.

Meaningful Click-Points:

The PCCP algorithm invites users to select a click-point sequence that has meaning or personal importance for them. In order to do this, points may be chosen according to distinctive elements in the picture, such as notable persons, places, or things.[8]

Usability and Memorability:

In order to enhance the password's usefulness and memorability, the PCCP system lets users choose click-points that have personal significance for them. People are likely to recall a series of events connected to a meaningful personal experience.[3]

Integrated Text Password, Image Recognition, and PCCP Multi-Factor Authentication

A. Text Password Authentication:

Users enter a standard text password as the initial authentication factor. The system checks the entered password against the stored credential database. If the password matches, the user advances to the subsequent stages of authentication.

B. Image Selection Authentication:

Upon successful text password validation, the system displays a set of images. Users choose specific images based on predetermined criteria or personal preferences. The system compares the selected images against the anticipated options to ensure authenticity before moving forward.

C. Click Points on Selected Images Authentication:

Once the user completes the image selection stage, they are asked to mark specific areas within the chosen images. The system records the coordinates of the clicked points and performs analysis to verify the user's identity.

The third step of the proposed three-step authentication system utilizes a technique called cued click points algorithm.[8] This method extends the concept of click points beyond simply selecting images to a more precise and targeted approach. Within this context, the cued click point's algorithm works as follows:

Algorithm:

Step-1.Text Password

Step-2: Image Selection:

The user is shown a collection of images, from which he has to choose a certain number of them. After then, a grid is created by dividing the chosen images to produce a matrix of clickable points.

Step-3: Point Selection: Users click on specific points within the image grid presented to them.

Step-4: Password Creation: the user as their password generates a sequence of click points.

Feedback Mechanism: Immediate implicit feedback is provided to user based on their click points.

Security Measure:

The security measures implemented in the graphical password authentication project using Cued Click Points (CCP) to protect user data and prevent common vulnerabilities like MySQL injection and XSS attacks include:

• Second-Level Key Click-Point Approach:Security is improved by implementing a second-level key click-point approach, which enhances the system's resistance to attacks. This approach adds an extra layer of security to protect user data.

• Alerts for Unauthorized Attempts: In case of unauthorized attempts, the system sends email notifications to users without revealing the hacker's identity.This proactive measure helps users stay informed about potential security risks and unauthorized access attempts.

• Warning Messages for Incorrect Click Points:If a hacker attempts to crack the system and enters incorrect click points three times, a warning message is delivered to the user's mobile device to alert them. This feature helps prevent unauthorized access and enhances the system's security.

The user interface design collaborates closely with security measures to create a seamless and secure authentication system. Design considerations may include implementing secure login screens, encryption protocols, and multi factor authentication options within the graphical password interface. The design should prioritize security without compromising usability, striking a balance between user experience and system protection. In conclusion, the user interface design approach to graphical password authentication is centered on developing an interactive, safe, and aesthetically pleasing interface that efficiently assists users in setting and entering graphical passwords. The user interface design is essential to the success of the graphical password authentication system since it integrates visual representation, interaction design, feedback mechanisms, accessibility features, and security integration.

In Password creation phase, user is given two options; user can either provide images of their choice or can select images from system database. In either of the choice user is required to provide three images. System uses distortion technique in Distortion phase to distort received or the provided images. This distortion of images is carried out by using filters. System then displays both the distorted and original images to the user; so that it is easier for user to mentally associate the distorted images. User is also required to enter some random text for each of these images. Both original and distorted images along with the text are saved or preserved in database. During Authentication phase, only valid user is or will be granted access to the system. The system will ask the user to identify one out of three user entered images from the grid containing one correct image and 8 decoy faces and also entering the associated text. User gets only two attempts to identify correct images from the grid and to enter the associated text of the image. The system shuffles the images in the grid every time the user logs in to the

Authentication: Users have to recreate their passwords during the login procedure by clicking on the designated places in the right order. If the sequence falls within the predetermined tolerance, the system validates the clicked locations against the password that has been saved. This approach[12] increases the precision and difficulty of the authentication process, thereby improving security. Additionally, the cued click point's algorithm can be adapted to accommodate various image types, sizes, and content, providing flexibility and versatility across diverse applications.

The objective of the project is to give users an easy-to-use and memorable authentication procedure. The system aims to improve overall authentication system usability by adding graphical features and cued click points. This project's increased usability is the result of a diverse strategy that emphasizes on the user experience and making sure the final product is effective and user-friendly. Through the application of user-centered design and usability principles, the project seeks to develop a system that efficiently accommodates the requirements and preferences of its users. The usability objectives—usefulness, effectiveness, learnability, and attitude (likeability)—must be taken into account in order to achieve improved usability. These aims guarantee that customers may accomplish their goals with the product in a simple, effective, and error-free manner. By giving these usability goals top priority, the project hopes to improve user happiness and experience as a whole.[3] The project also highlights how crucial it is to create user-product interfaces that are simple, easy to use, intuitively logical and organized, affordance, mapping, constraints, visibility, and low memory burden. These features guarantee that users may interact with the system in an intuitive

manner, free from needless complexity or ambiguity, which improves the user experience.

Confidence scores derived from the cued click point's algorithm can be combined with other authentication factors to generate a cumulative trustworthiness metric for the user's identity. This holistic assessment ensures a higher level of security and reduces the possibility of false positives or false negatives.

The development and deployment of a novel authentication system that makes use of cued-recall graphical password techniques is included in the project scope on graphical passwords utilizing Cued Click Points (CCP). By letting users click on one point per image for a series of photos, each image being predicated on the preceding click-point, the project seeks to improve security and usability. This method includes visual indicators that notify legitimate users in the event that they enter their last click-point incorrectly, in addition to giving consumers rapid feedback during the authentication process. The new software development project's compatibility with the current infrastructure and systems is the first thing the project does. Before moving further with the integration process, this phase makes sure that any compatibility concerns are resolved. Subsequently, an extensive evaluation of the existing infrastructure is carried out to pinpoint its shortcomings and potential areas for enhancement. As part of this research, server capacity, network setups, scalability, and possible failure points are assessed.

Quality assurance for graphical password authentication involves ensuring the security and effectiveness of graphical password schemes through empirical evaluations. Studies have shown that user-chosen graphical passwords can have lower entropy and be correlated with user characteristics, potentially compromising security. This highlights the need for a different approach to password selection in graphical schemes compared to text passwords. By evaluating user-chosen graphical passwords and considering factors like user choice and scheme design, quality assurance aims to enhance the security and usability of graphical password authentication systems.

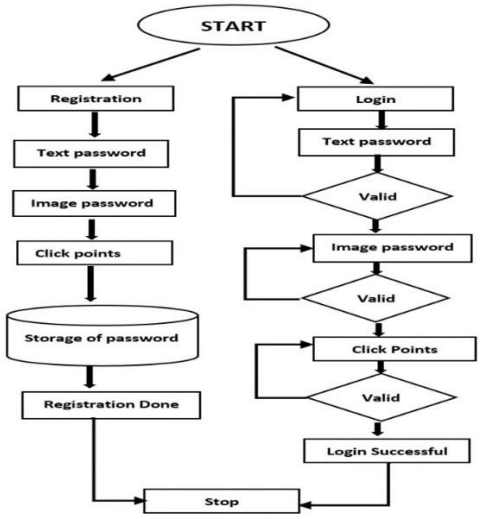

Figure 1: Flowchart Diagram

Developing a graphical password authentication system that is resistant to shoulder-surfing attacks is another important goal. The project's goal is to counter security risks such as passwords being directly observed or recorded by unauthorized parties by introducing novel approaches and ideas. In this project, an innovative graphical password strategy that prioritizes security enhancement without sacrificing usability is implemented to prevent shoulder-surfing. Rather than clicking on their password images, users of the proposed technique must draw a curve across them in a certain order. This drawing input technique greatly lowers the likelihood of shoulder-surfing attacks by human observation. It is modeled after the DAS drawing input and association mnemonics in Story for sequence retrieval.

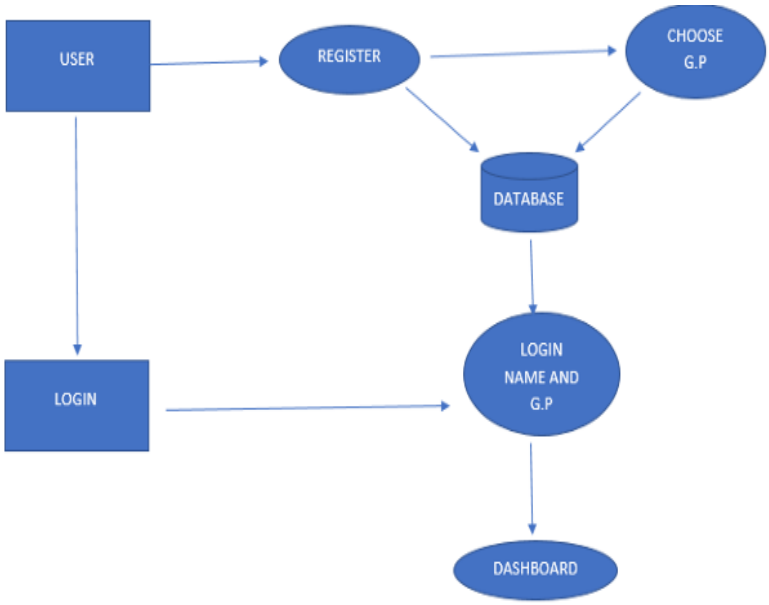

Figure 2: System Architecture

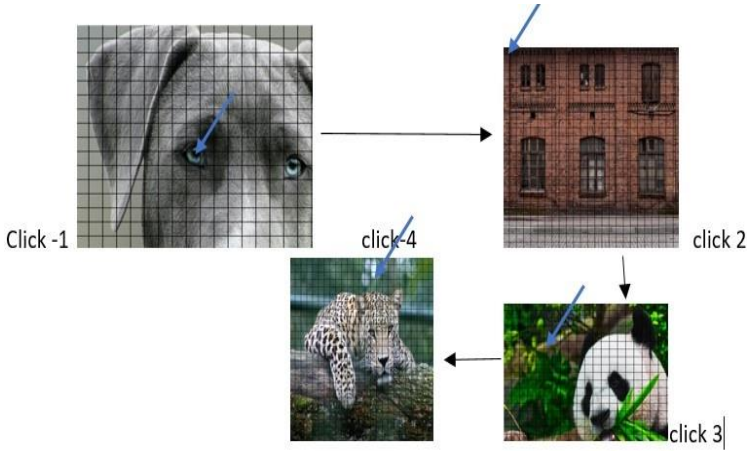

Figure 3: The user in CCP chooses one click point for each image. The current click point determines the next image displayed.

4. RESULTS:

Combining text passwords with graphical passwords [12] offers significant advantages in terms of security and usability. By incorporating both text and graphical components, authentication systems can leverage the strengths of each approach to create a more robust and user-friendly solution[12].When a person uses graphical input and output devices (such a mouse, stylus, or touch screen) to enter a secret into a computer, that secret is known as a graphical password. A Graphical Password can be made by combining images or photographs. Stated otherwise, a graphical password is an authentication mechanism that makes selections from a set of images presented in a prearranged order within a graphical user interface (GUI). For this reason, the graphical-password technique is also known as graphical user authentication (GUA). [1]

Improved security: Graphical passwords are generally more resistant to dictionary attacks and phishing attempts compared to text-based passwords. When combined with text passwords, the resulting authentication system becomes less susceptible to common password attacks.

Enhanced usability:Because people tend to correlate visual cues with memories more easily than text-based ones, graphical passwords are frequently easier to remember.By complementing text passwords with graphical ones, users can enjoy a more intuitive and engaging authentication experience.

Reduced vulnerability to attacks:Users can reduce the risks associated with popular password attacks, such as brute-force and phishing attempts, by combining text and graphical passwords.Graphical passwords can provide benefits over alphanumeric passwords in terms of memorability and resistance to certain types of attacks.

Greater flexibility: The combination of text and graphical passwords allows for a broader range of authentication options tailored to meet the needs of various user groups and application scenarios. Three-step authentication strikes a balance between strong security and user convenience, offering a more robust and accessible authentication experience. A traditional text password serves as the primary means of authentication, requiring the user to recall a unique sequence of characters known only to them. Selecting specific images from a given set introduces a possession factor, where the user demonstrates control over a physical object (the images themselves) during the authentication process. The cued click point's algorithm adds an inherence factor by asking the user to perform specific interactions with images, thereby confirming their presence and ability to execute the action.

A discretization algorithm is applied during password construction to get the matching grid and tolerance square of a click-point. This grid is downloaded and utilized for each click-point in a subsequent login attempt to see if it is within tolerance of the originating point. The user also need to decide which next image to display with CCP. The project implements a compelling feature, using CCP as the foundation system, to entice users to choose passwords with higher levels of security and to make it more challenging to choose passwords with all five click-points serving as hotspots.[12] A graphical password system variation called Cued Click Points (CCP) aims to improve both security and usability. When it comes to graphical password systems, CCP has several benefits over the others. [8]

Improved security: Graphical passwords are generally more resistant to dictionary attacks and

phishing attempts compared to text-based passwords.When combined with text passwords, the resulting authentication system becomes less susceptible to common password attacks.

Enhanced usability: Graphical passwords are often easier to remember than text-based passwords, as humans can more readily associate visual cues with memories. By complementing text passwords with graphical ones, users can enjoy a more intuitive and engaging authentication experience.

Reduced vulnerability to attacks: By combining text and graphical passwords, users can mitigate the risks associated with common password attacks like brute-force and phishing attempts.Graphical passwords can provide benefits over alphanumeric passwords in terms of memorability and resistance to certain types of attacks.

Greater flexibility: The combination of text and graphical passwords allows for a broader range of authentication options tailored to meet the needs of various user groups and application scenarios.

Three-step authentication strikes a balance between strong security and user convenience, offering a more robust and accessible authentication experience

Cued Click Points (CCP) is an alternative to PassPoints. In CCP, users click one point on each of three images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images. For implementation, CCP initially functions like PassPoints.

Each image requires a single click: To minimize cognitive burden and error-proneness, CCP encourages users to click just once on each image, in contrast to PassPoints that demand users to pick five click points on a single image.

Instant feedback: The following image appears as soon as a user clicks on one, providing constant direction and feedback.

Decreased hotspot risk: Because users only click once on each image, there is less likelihood that they would produce recurring patterns, or "hotspots," which exacerbate password cracking.

Ease of use: CCP encourages users to select more random and complex click points, making it easier to adopt and implement compared to other graphical password schemes.PassPoints, like text passwords, may only securely offer feedback at the conclusion and cannot identify the root of an error. While CCP's visual cues should not aid attackers in this way, giving clear feedback in PassPoints prior to the last click-point would enable PassPoints attackers to launch an online attack to reduce viable password subspaces. The fact that recalling a single point from each of five photographs is cued to be easier than memorizing an ordered sequence of five points from a single image-utilizing algorithm is another boost in usability.

Figure 4: User need to select points on the image to create password.

Select Point On Image To Create Your Password

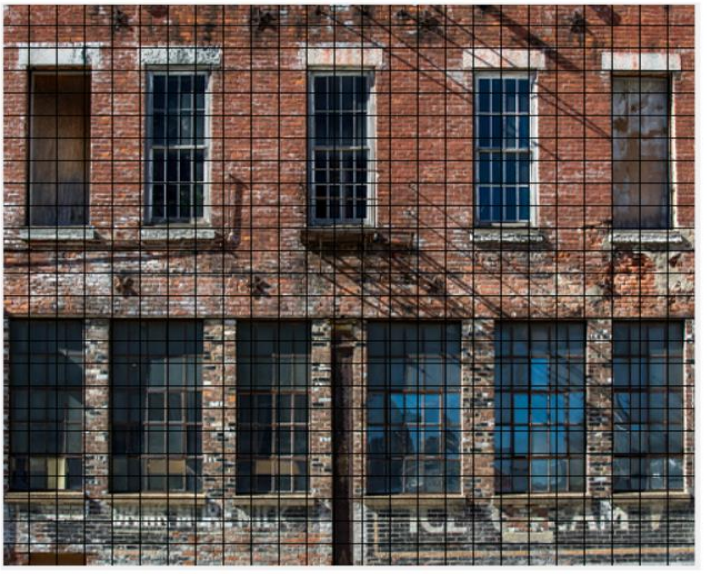

Figure 5: User need to select points on the image to create password.

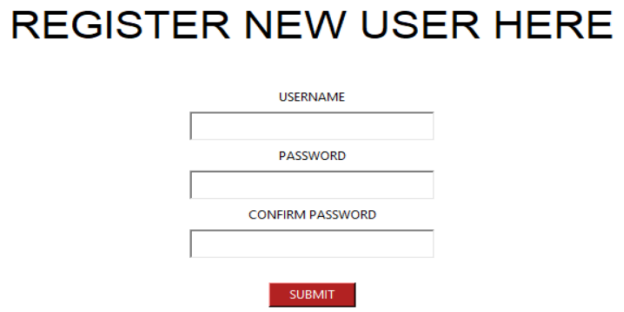

Figure 6: User need to enter a text password as first phase of registration.

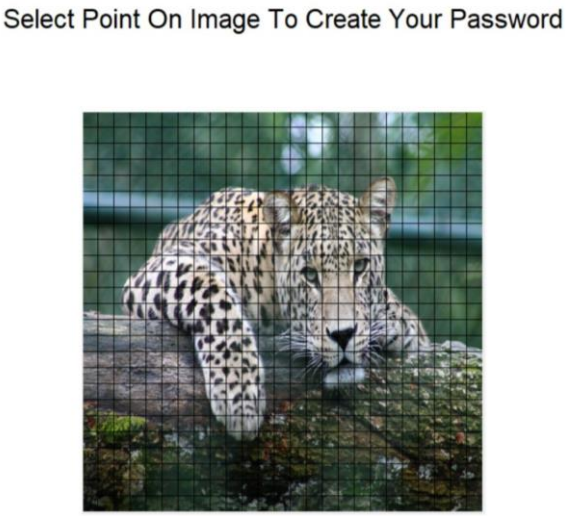

Figure 7: User need to select points on the image to create password.

5. CONCLUSION:

In an era where cybersecurity threats are ever evolving, the need for robust and user-friendly authentication systems has become paramount. The project at hand aims to address this challenge by proposing a novel three-step authentication system that combines traditional text passwords with graphical elements. By integrating both types of passwords, this system seeks to enhance security while ensuring a seamless user experience.

Using images as passwords instead of alphanumeric ones is becoming more and more popular. The primary justification for utilizing graphic passwords is can be quickly remembered. This document includes suggested graphical password authentication with two steps mechanism

that utilizes Pass faces. To create our system is both user-friendly and concurrently, the project is a blend of text and visuals to make it more challenging to break. The original pictures that the user took are whether it is susceptible to unique informed guess assaults users have a lot of knowledge regarding the people. Additionally, even in the absence of any user knowledge, attackers are still capable of making better assumptions than random assumptions depending on the context of the original images.Adding more photographs to the system enables attackers to arbitrarily raise the workload on CCP targets, which suggests that CCP offers better security than Pass Points. [7] [8]

The use of graphical password authentication systems offers an encouraging substitute for conventional methods that rely on alphabetic input. These systems try to increase security while enhancing user experience and memorability by using images as passwords. Nevertheless, the adoption and execution of graphical password systems raises a number of issues and concerns. Because visuals are easier for the human brain to recall than alphanumeric characters, graphical passwords have the distinct advantage of being rapidly recalled by users. Furthermore, security is improved without sacrificing usability when meaningful click-points are used, as the suggested Cued Click Points (CCP) method demonstrates. Different authentication techniques are incorporated into the multi-layered approach, which further increases security by mixing text and image-based passwords.

Graphical password schemes do have some disadvantages, though. Usability problems and shoulder-surfing attacks are still concerns that need to be addressed with continued research and innovation. Furthermore, the Human-Computer Interaction (HCI) and security communities continue to face a formidable problem in building authentication systems that strike a balance between security and usability. Notwithstanding these difficulties, graphical password authentication solutions have a great deal of promise to raise digital systems' general security posture while boosting user satisfaction. With further study and improvement, these methods may replace or supplement conventional text-based passwords as a common authentication mechanism in a variety of applications

Using text passwords or graphical passwords alone can present inefficiencies and security vulnerabilities. Text passwords are susceptible to brute-force attacks, dictionary attacks, and password reuse issues, while graphical passwords may suffer from predictability, shoulder surfing, or smudge attacks. However, combining these two [12] authentication methods in a unified system can offer significant benefits. By integrating text passwords for their familiarity and ease of use with graphical passwords for their visual memorability and resistance to certain types of attacks, organizations can create a more robust authentication system. This combined approach leverages the strengths of both methods to enhance security and usability, providing users with a more secure and user-friendly authentication experience. The integration of text and graphical passwords in a combined system not only addresses the inefficiencies of using them individually but also offers a balanced approach that strengthens overall security measures while maintaining user convenience.

Collaboration between researchers, industry experts, and user feedback will be pivotal in shaping the evolution of graphical password systems. It is vital to continuously address ethical considerations, privacy concerns, and the need for robust and effective user training will be essential for widespread adoption. In summary, future enhancements in graphical password

authentication systems should focus on strengthening security, enhancing user experience, exploring innovative approaches, and conducting ongoing research and collaboration. By addressing these areas, the goal is to create more secure, user-friendly, and adaptive authentication systems for the future. The proposed Cued Click Points methodology has the potential to be a useful and memorable authentication solution. Because it leverages users' visual recognition abilities and the memory trigger that displays when they view a new image, CCP is more intuitive to use than Pass Points. Rather to having to learn an ordered series of clicks on a single image, it seems easier to be cued when each image is displayed and only need to recall one click-point per image (CCP). In conclusion, the project's integration of text passwords with cued click points in a three-step authentication system demonstrates a secure and user-friendly approach. By utilizing Python libraries like Tkinter and Pickle, the project successfully implements a robust authentication framework. The methodology of selecting click points within images for graphical passwords proves effective in enhancing security and usability. This innovative combination offers a promising solution to traditional password vulnerabilities, showcasing the project's potential in improving authentication processes.In conclusion, CCP provides increased security by making it harder for attackers to succeed, adding additional security layers via image-based authentication, and making the authentication process more difficult and involved than with conventional techniques. Through the utilization of interactive components and visual signals, CCP enhances the overall security posture of authentication systems, fortifying them against a range of cyber threats and attacks.

Future developments in graphical password authentication systems ought to concentrate on resolving current issues and investigating novel strategies to improve both security and usability. User feedback, industry professionals, and researchers working together will be essential in determining how graphical password systems develop. Enhancing security measures to mitigate shoulder-surfing attacks and other potential vulnerabilities. Improving usability through user-centered design principles and adaptive authentication methods.

Exploring novel approaches, such as biometric authentication and context aware authentication, to further enhance security and user experience. Conducting ongoing research and collaboration to stay abreast of emerging threats and technological advancements in the field of graphical password authentication. Standardizing graphical password authentication protocols and frameworks to ensure interoperability and compatibility across different platforms and systems. Educating users about the importance of strong graphical passwords and best practices for creating and managing them securely. Future developments in graphical password authentication systems have the potential to completely transform digital security. Future research may investigate cutting-edge technologies like artificial intelligence and machine learning to strengthen security measures in addition to the suggested improvements. By allowing systems to adjust dynamically to new threats and user behaviors, these technologies have the potential to improve the overall security of graphical password authentication.

Additionally, integrating blockchain technology may provide decentralized and impervious to tampering authentication solutions, hence strengthening the security of graphical password systems. More thorough and user friendly authentication processes may result from ongoing research on biometric authentication modalities like face recognition and iris scanning. The

potential for graphical password authentication systems to create a safe, user-friendly, and technologically advanced digital authentication landscape is enormous if these creative techniques are adopted and collaboration between different disciplines is encouraged.The intention is to close the gap between security and usability in graphical password authentication by tackling these issues and developing more adaptable, safe, and secure authentication systems in the future.

References

1. A. Abraheem, K. Bozed and W. Eltarhouni, "Survey of Various Graphical Password Techniques and Their Schemes," 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya.
2. G. Agarwal, S. Singh and A. Indian, "Analysis of knowledge based graphical password authentication," 2011 6th International Conference on Computer Science & Education (ICCSE), Singapore, 2011.
3. H. Adamu, A. D. Mohammed, S. A. Adepoju and A. O. Aderiike, "A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication," 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 2022.
4. ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "Graphical Password Authentication"- Cloud securing scheme," IEEE 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
5. Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science, Georgia State University, Dec-2005, IEEE
6. J. G. Kaka, O. O. Ishaq and J. O. Ojeniyi, "Recognition-Based Graphical Password Algorithms: A Survey," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021.
7. G. -C. Yang, "PassPositions: A secure and user-friendly graphical password scheme," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, Indonesia, 2017.
8. S. Kaja and D. Gupta, "Graphical password scheme using persuasive cued click points," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bengaluru, India, 2017.
9. D. E. Vieira, T. L. M. Abreu, M. E. V. Melgar and L. A. M. Santander, "A cued-recall and emotion classification graphical password authentication scheme," 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), Cartagena, Colombia, 2017.
10. M. Singh, V. Nedungadi and R. Radhika, "A Hybrid Textual-Graphical Password Authentication System with Enhanced Security," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023.
11. A. H. Lashkari, R. Saleh, F. Towhidi and S. Farmand, "A Complete Comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009.
12. A. M. Joshi and B. Muniyal, "Authentication Using Text and Graphical Password," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018.