SecureWeb : Elevating Web Authentication with PCCP and Email-Driven OTP

MSc Research Project
Cyber Security

Sriram Kalyanasundaram
Student ID:21246734

School of Computing
National College of Ireland

Supervisor: Rohit Verma

National College of Ireland
Project Submission Sheet
School of Computing

x21246734@student.ncirl.ie

Student Name:	Sriram Kalyanasundaram
Student ID:	21246734
Programme:	MSc in Cyber Security
Year:	2023
Module:	MSc Research Project
Supervisor:	Rohit Verma
Submission Due Date:	31/1/2024
Project Title:	SecureWeb : Elevating Web Authentication with PCCP and Email-Driven OTP
Word Count:	6603
Page Count:	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Sriram Kalyanasundaram
Date:	31st January 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

SecureWeb : Elevating Web Authentication with PCCP and Email-Driven OTP

Sriram Kalyanasundaram

x21246734

Abstract

Websites are revolutionizing today's world as everything is getting devitalized. From Security perspective, this digitization is not only limited to a positive impact, but a negative impact as well, since the number of cyber-attacks is increasing at an alarming rate with evolving Cyberthreats, strong authentication systems are in high demand. The innovative proposal of this paper is merging 'Persuasive Cued Click Points' (PCCP) authentication and email-based verification authentication method. PCCP authentication method is a unique, memorable pattern for users, improving security and usability in graphical password systems. As an additional security layer, Email based OTP is introduced where random three-digit binary opt is sent to the user using SMTP protocol. Based on the OTP the user will select the points on the images and login. The proposed system prototype is assessed on the basis of user experience and security. In Summary, a strong and convincing method for improving the authentication methods for websites and application is proposed in this paper. Evaluation of the model is done based on the valuable feedback of the participants after using the web prototype

Keywords: PCCP-E, Authentication, Cyberthreats, SMTP

1 Introduction

In the ever-evolving realm of cyberspace, where our daily interactions, transactions, and communications increasingly occur online, the role of robust web authentication methods cannot be overstated. The digital age has brought forth an array of cybersecurity challenges. The need for secure, yet user-friendly, methods of verifying identities and safeguarding sensitive data has propelled researchers and cybersecurity professionals to explore innovative authenticating system. Among these, "Persuasive Cued Click Points" (PCCP) has emerged as a captivating approach that intertwines elements of human psychology, graphical design, and cybersecurity to redefine how users prove their digital identities. PCCP-E is a potential strategy with combining PCCP where the input for these will be based on the OTP that is received through email. PCCP-E makes use of the patterns and visuals which are recognised by the user's cognitive ability which is automatically immune to common cyber-attacks that target traditional text based password. A multilayer process is involved here as the images are selected based on the OTP that is received in the email which adds an extra layer of security to the model. Most of the paper talks about the security aspects of this method hence this paper will focus on user-experience and security. A survey with a set of questionnaires was carried out to capture the user perspective over the login prototype.

1.1 Web Authentication and Types

The basic procedure by which people prove their identity in order to access online materials, platforms, or services is known as web authentication. The conventional approach requires users to enter a username (Identifier) along with a secret passphrase. The difficulty of creating and remembering complicated passwords for users and the susceptibility of passwords to different cyberthreats are just two of the many obstacles that this strategy has had to overcome. Multi-Factor Authentication (MFA) has become a reliable solution to deal with these problems. MFA demands multiple forms of identity from users, usually combining knowledge-based forms (like passwords), possession-based forms (like smartphones or security tokens), and identity-based forms (biometric data, like fingerprints or facial recognition). Through the mitigation of authentication with one factor risks, this layered approach considerably enhances safety J (2020 Jul 8).
A subset of MFA called biometric authentication employs a person's distinctive physical or behavioural characteristics to confirm their identity. An extremely safe and convenient authentication process is offered by technologies like voice recognition, iris scanning, facial recognition, and fingerprint recognition. Nevertheless, there might be difficulties like the requirement for specialised hardware, possible false positives and installing them everywhere is not feasible. Adaptive authentication mechanisms provide a more flexible and responsive security framework by adjusting the required level of authentication based on the perceived risk. Password less authentication is a relatively new trend that seeks to completely do away with the need for conventional passwords. Rather than relying on password-related assaults, users could authenticate using alternative methods like biometrics, one-time codes, or secure authentication tokens. In conclusion, web authentication is a field that is always developing in response to the dynamic nature of cyberthreats. Employing a mix of these authentication techniques, organisations can develop a flexible and all-encompassing approach that puts security and user experience initially.

The security procedure known as website authentication enables users to confirm their true identities before being granted accessibility to their private accounts on a website. When a user logs into any sort of internet-based account—be it networking sites, online shopping, incentives, banking on the internet, or perhaps something else entirely—this process goes on in the background. A user generates a unique identification and key when they register for an initial account on a website; these could be needed later to authenticate their identity and grant access to the consideration again. After that, the user identification and key are kept on file in an extremely safeguard web server so they could be compared to future login information. The concept revolves around granting exclusive access to user accounts through personalized IDs and keys, ensuring that only the rightful user possesses the means to enter their account. Identification and authentication methods vary widely, ranging from vulnerable set-ups susceptible to attacks to highly secure processes. Despite the prevalence of the conventional username and password combination as the standard ID and key, these traditional schemes have faced growing vulnerabilities to cyberthreats. Fortunately, contemporary alternatives offer enhanced security measures and improved user experiences, providing a more robust defence against

potential attacks.
Implementing robust authentication system on the website is crucial for maintaining a secure and user-friendly online environment. Inadequate authentication processes pose the risk of unauthorized individuals gaining access to sensitive user data, a concern particularly evident in traditional username/password authentication methods. Data breaches not only jeopardize the privacy of individual users but can also inflict severe damage on your business or organization's reputation and financial standing. When developing or updating website authentication systems, it's essential to prioritize two key factors: user experience (UX) and security. While website authentication may initially appear complex but it is manageable to implement. Acquiring a clear understanding of the process can significantly contribute to ensuring the adoption of the most effective and secure practices. Step 2 of the procedure is mostly to blame for the confusion surrounding website authentication. As was already mentioned, there are numerous ID types and key combinations that people could utilise to access their accounts; each has advantages and disadvantages of its own.

1.2 Integrating PCCP with Email for Enhanced Security

PCCP departs from the conventional reliance on alphanumeric passwords, introducing a novel graphical password scheme. At its core, PCCP leverages the human brain's innate ability to recall spatial and graphical information more effectively than complex character sequences. During the registration process, users are prompted to select specific point on an image, creating a unique and personalized authentication sequence. This departure from the traditional text-based approach aims to enhance both the security and memorability of user credentials, aligning with the evolving demands of modern digital interactions Ghiyamipour (2021). However, recognizing that no single authentication method is foolproof, the integration of PCCP with email-based authentication emerges as a holistic strategy to fortify the web's security architecture. Email, all over in its role as a primary communication channel, takes on new significance beyond its traditional functions. It becomes a secondary layer of identity verification. By merging the graphical and interactive strengths of PCCP with the established reliability of email-based authentication, this integration seeks to create a strong defence mechanism against an array of cyberthreats. In the upcoming exploration of the PCCP with email-based authentication, our objective is to dissect and comprehend the nuanced intricacies of this innovative combination. We go deep into the individual strengths and potential vulnerabilities of each component, aiming to construct a comprehensive understanding of how this relationship contribute toward a more secure, user-centric, and adaptable web authentication system.

The combination of email-based authentication and Persuasive Cued Click Points (PCCP) represents a sophisticated and all-encompassing method of strengthening the web security environment. Fundamentally, the goal of this integration is to combine the flexibility and dependability of email verification with the graphical strength of PCCP to create a multifaceted authentication system. Email verification is the cornerstone of this integration; it is an essential step integrated in user registration procedure. This step establishes the validity of the user's identity in addition to verifying the authenticity of the email provided by sending a special verification binary code to the registered email address of the user. Multi-Factor Authentication (MFA) Ometov et al. (2018) is seamlessly integrated into the authentication process as the integration progresses. The design, however, goes one step further and requires the entry of a one-time code that is emailed to the user's registered email address. This adds another level of verification. This dualistic approach to authentication factors not only improves the security posture overall, but it also fits with the current focus on multi-layered defences against cyberattacks. The technique reduces the vulnerabilities associated with conventional single-factor authentication by fusing the possession-based confirmation of email with the spatial and graphical memory strengths of PCCP.

It smooths the transition between graphical elements and email verification, supporting both strong user authentication and user experience. The mutually beneficial connection between email authentication and PCCP offers a novel and flexible approach to the problems associated with online identity security, leveraging the advantages of both email-based verification and state-of-the-art image authentication.

1.3 Research Question

Can Integrating PCCP with Email Authentication contribute to better user experience and security in web authentication ?

1.4 Research Objectives

- To evaluate PCCP-E's performance in improving user authentication on web platforms as a graphical password scheme.
- To assess user acceptability and usability, evaluate PCCP-E in comparison to conventional password-based authentication techniques.
- To evaluate how PCCP and email verification work together to improve the overall security and usability of the authentication process.

2 Related Work

Web authentication techniques are essential for protecting digital communications and guaranteeing the privacy, confidentiality, and integrity of user data. The security landscape is constantly evolving due to technological advancements, which is why researchers are constantly looking for new ways to reduce risks. This review of the literature sets out to explore the corpus of research on web authentication techniques in order to identify the advantages and disadvantages of popular approaches. It establishes the foundation for a more sophisticated and successful authentication method by pointing out the flaws and restrictions in the existing methods. The following sections explore the state of art web authentication techniques today, explain their shortcomings, and review the literature on PCCP principles' application, providing a thorough overview of the field of study.

2.1 Web Authentication Methods

Within a subsection of internet safety called Authentication, Cued Click Points (CCP) is a visual authentication of passwords methodology. The procedure by which an application confirms the identity of an individual is called authentication. A form of authentication known as a "visual password" involves an individual to choose pictures from an interactive user interface in a specific sequence. Visual passwords serve as a backup for plain alphanumeric credentials. Although difficult to determine, graphic passwords are simple to establish. Assisting clients in choosing a stronger password increases security and is a key objective of systems authentication. Clicking on a single point inside an image sequence is how users interact with Cued Click Pointer. Relying on the prior click-point, the subsequent image would be shown. Acceleration, precision, and the quantity of mistakes are all improved. Although the series of visuals makes an attacker's operation more difficult as Cued Click Points (CCP) offer exceptional protection. The effectiveness and safety of login information would increase as the number of grids and images increases. But while outstanding safety and high reliability are necessary to build an effective system, simplicity accessibility cannot be separated from it. One of the disadvantages that is not addressed is shoulder surfing which might lead to observing the click points which led to cracking the CCP Sunil et al. (2014).

A study on the use of face images as a password alternative was carried out by Brostoff, S., and Sasse (2000) with 32 participants. Here the human face is used as a password. There were two drawbacks to this method: shoulder surfing and a survey conducted by Davis et al. (2004) revealed that the user's gender, race, and facial features all affected the face selection. A bad process outcome will result if someone is uncomfortable with the face, they are shown Brostoff and Sasse (2000)
The contemporary digital landscape, the significance of robust password security cannot be overstated. Various techniques are available for password protection, among which Cued Click Points stand out as a click-based graphical password scheme employing a cued-recall technique. Users interact with a sequence of images by clicking on specific points rrecognizing the inherent challenge of users opting for easily memorable passwords, which may be susceptible to guessing by attackers, the study focuses on evaluating the usability and security of a graphical password authentication system using Cued Click Points. The system aims to enhance usability by guiding users toward selecting more secure passwords, thereby expanding the effective password space and increase in security. The introduction of hotspots is attributed to poorly chosen passwords, and the click-based graphical password system encourages users to choose for more random and intricate click-points, making the passwords harder to guess. It's worth noting that the study's scope may not fully encompass user preferences potentially limiting the generalizability of findings across diverse user populations Moraskar et al. (2014).

Alphanumeric usernames and credentials represent the prevalent computer authentication method, but this approach exhibits notable drawbacks. Users often choose easily guessable passwords, while more complex passwords become challenging to remember. However, existing graphical password systems are susceptible to shoulder surfing attacks. To address this vulnerability, this study introduces a web-application authentication system based on visual cryptography and cued click point recall-based graphical passwords. The system's efficacy was validated through unitt system, and usability testing, with results indicating successful achievement of objectives and requirements. Usability testing further affirmed the system's user-friendly nature and high security. Nevertheless, real-world applicability may encounter challenges related to user acceptance and integration into existing web-application frameworks, aspects warranting further exploration beyond the scope of this study Kenneth and Olujuwon (2021).

The literature under discussion delves into several facets of authentication systems, primarily emphasising graphical password approaches. Cued Click points (CCP) are a noteworthy technique wherein users click on particular spots within a series of images, thereby raising the workload for possible attackers and improving security and performance. In order to increase security against various attack scenarios and to improve memorability and usability, projects combine graphical passwords into SMS file transfers and provide hybrid authentication techniques. Furthermore, a system of authentication that employs visual cryptography seeks to address problems related to shoulder surfing. Additionally, a fingerprinting-based identification technique that makes utilisation of canvas problems is demonstrated, proving to be resilient against replay assaults and highlighting the significance of creative solutions for improving web security. One of the drawbacks is integrating a fingerprint sensor to a prototype is not feasible.

2.2 PCCP principles and their application in enhancing data security

User authentication is an essential part of security for computers, performing a critical role in protecting resources and systems. Authentication, an essential area of security studies, involves assessing if a person should be allowed entry to a certain network or service. This procedure is employed by an application to verify and authenticate the identification of an individual. However, one significant difficulty is that consumers often employ credentials that are readily guessable. The login information that has been constructed to be impossible to determine, on the other hand, might be tough for users to retrieve. In response to the challenges associated with traditional text passwords, researchers have introduced innovative authentication methods utilizing images as passwords, commonly known as graphical passwords. Graphical passwords operate by incorporating images for user login, enhancing both usability and memorability. Distinct categories of graphical passwords have emerged, distinguished by the nature of memory retrieval—namely recall, cued-recall, and recognition. Despite the variety of graphical password options available, the chosen implementation of this paper focuses on the Persuasive cued click-based approach. Cued click points represent a click-based graphical password scheme where users select specific points on a sequence of images. The subsequent image is dependent on the click point chosen in the previous step. The system exhibited commendable performance, excelling in terms of speed, accuracy, and minimizing errors. Graphical passwords present a promising avenue for enhanced security compared to traditional text-based counterparts. This advantage arises from the common practice among individuals of using plain words, rather than the recommended complex character combinations, to memorize text-based passwords. Despite their advantages, graphical passwords are not without limitations and face issues similar to those encountered by other graphical-based password systems such as shoulder surfing Saha et al. (2019).

Currently, a crucial method of ensuring privacy is identification technologies. The most popular verification technique is an alphanumeric login address and password. Users usually select easy-to-guess credentials that are notable but system-assigned passwords are challenging for users to recall. Researchers introduce a visual pass-code that is safe from shoulder surfing attacks and depends on cued recall. Additionally, researchers suggest an image encryption method that makes utilisation of a two-dimensional cat mapping and an edge recognition technique that determines an image's boundary by fuzzy logic interpretation. Following that, thee approach encrypts the user credentials before putting it in the repository. The suggested solution performs well in terms of security and usability, according to experiments. Shoulder surfing assaults are possible due to the unsuitability of these credentials in locations with Surveillance or password-capturing capabilities Ghiyamipour (2021).

In the current situation, security is the first priority. The requirement for safeguarding information presents unique challenges to cyber security team. The main purpose of user-chosen passwords is to enable system authentication. Most customers create memorable passwords that are simple to guess and are vulnerable to hacking attempts. Visual passwords based on identification are safe against capturing, speculating, and surfing the shoulder assaults. The method for defending from an overhead surfing assault is presented in this paper. The strategy relies on an image matrix in which the individual using it provides his username before identifying the password images. The pictures are sorted so that any column or row without a password is removed. Nevertheless, in order to guarantee the dependability and applicability of the suggested security solution, the efficacy of the defence against shoulder surfing attack must be further verified through rigorous testing, including real-world scenarios Kathole et al. (n.d.).

Unlike traditional typed passwords, graphical passwords involve selecting images or sketching symbols as a means of authentication. They offer a potential solution for addressing issues with text-based password systems. It is suggested that guessing or hacking graphical passwords is more challenging than regular ones. This paper suggests a way to log in using pictures instead of words or numbers. The new system calculates the password strength using math and keeps the password secure using a special code. The intended system has been transformed into an android application. The length of time for logging in, the strength of the password, and its complexity were all evaluated based on previous research. The results show that the new system is better than the old one. It has a faster login time and gives more accurate results. However, the selection of password options is limitedAbbas and Jawad (2023)

It is important to have robust security measures in place to safeguard the privacy of users' personal information. The paper introduces an innovative approach for users to verify their identity when using a computer. The design aims to provide a balance between security and user-friendliness. By combining recognition, memory, and cues, they have enhanced the security system beyond others. The CS-AV symbols are used together to create a password system known as Captcha. Users can draw a shape or pattern on a grid to enter a password. Utilizing the CS-AV and grid cells allows for a broad range of passwords to be easily managed. This finding was discovered in research on memorable passwords. The new plans will work on most input devices and will protect your phone from people looking over your shoulder while you unlock it. One potential issue with the new picture password system is that users may have trouble recalling intricate patterns. Expanding the password space may actually present challenges for individuals trying to access their accounts Khan and Chefranov (2020).

The rapid expansion of the Internet structures and the utilization of sophisticated, large-scale applications have resulted in a growing requirement for the design and implementation of multifeatured networking applications. The Argumentative Cued Click-Points visual username and password system is evaluated holistically in this paper, taking into account execution factors, safety and ease of use assessments. Supporting individuals in choosing login credentials with a higher level of security—that is, ones that fall within a wider range of efficient security—is a crucial accessibility objective for based on expertise authentication mechanisms. In order to encourage individuals to choose fewer predictable, and therefore greater challenging to believe click-points, it utilizes persuasiveness to impact their choices in click-based visual passwords. Yet there hasn't been much success with offering tools like strength meters for usernames and passwords or directions on how to create strong login credentials and utilise password management programs Ameen et al. (n.d.)

Numerous studies addressing the crucial concerns about the functionality, security, and usability of authentication systems are included in the examination of the literature, with a special emphasis on graphical password schemes. Regarding feedback-led optimization and safety, real-time high-quality data on the functioning of digital health applications is prioritized. Although difficulties and ambiguities in the creation and validation have been recognized, patient- and clinician-reported consequences and high-quality surveys are thought to be crucial for obtaining data from actual situations. The limitations associated with conventional alphanumeric login and password methods—such as users selecting easily guessable passwords—are acknowledged, underscoring the significance of user authentication in computer security. Abbas and Jawad (2023) suggested the use of graphical passwords, more specifically the cued click points method, as a more effective and safe option. For ease of use and memorability, these graphical passwords take advantage of the picture superiority effect. The identification of shoulder surfing attacks as a possible danger to graphical passwords led to the creation of security-enhancing methods like grid-based image authentication. However, more thorough evaluation, such as real-world scenarios, is required to validate the efficacy of defence against shoulder surfing assaults. Khan and Chefranov (2020) addresses the difficulties in striking a balance between safety and ease of use, highlighting the requirement for authentication systems that assist users in creating passwords that are secure.

A variety of graphical password strategies are offered as substitutes for conventional text-based login credentials, including PCCP and Click Symbols Alphabet (CS-AV). It is investigated whether combining identification, re-called, and cued-recall-based schemes could enhance both safety and accessibility. The Android implementation, developed by Ameen et al. (n.d.) , depends on graphical password techniques and presents a method of computing password points through the utilisation of histogram computation, which is then encrypted for greater safety. Comparing this technique's assessment to other approaches, it performs better with regard to of entropy and logging delay. The examination of the research highlights how systems for authentication are changing, with a move towards visual passwords and an investigation of novel approaches to improve safety, accessibility, and practical efficiency. Nonetheless, difficulties and the requirement for additional verification of suggested remedies are constantly underlined in the examined research.

Chiasson et al. (2011) conducted research that introduces Persuasive Cued Click-Points (PCCP), a click-based graphical password system designed to improve password security without sacrificing usability by encouraging users to choose stronger passwords through persuasive techniques. Eight user studies were conducted on PCCP with text password and image-based methods. This proved that PCCP had a good login success rate and a recall rate in the experiment. It was found that malware interruption during user input and shoulder-surfing are some of the vulnerabilities of PCCP. The added novelty in this paper will eliminate the problem of shoulder surfing as the inputs will not allow to create a pattern as the input is based on the binary otp from the email.

3 Methodology

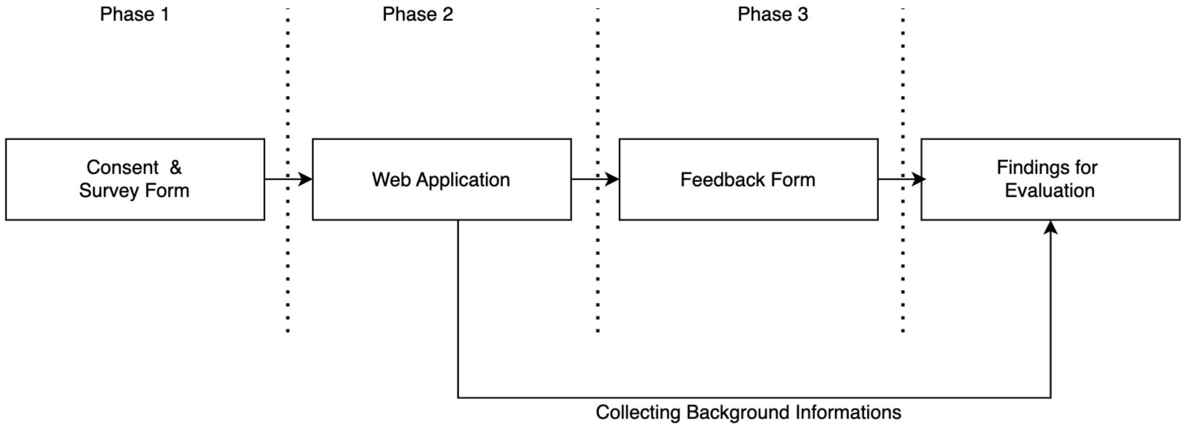

Figure 1: Research Project Flow

In the ever-evolving landscape of digital security, the need for robust authentication mechanisms has become paramount. Cyber threats continue to advance, making it imperative for organizations and individuals alike to adopt innovative solutions that safeguard sensitive information. In this context, our proposed methodology integrates Cued Click Points (PCCP) with an additional layer of security utilizing email input to create a resilient authentication model. To explain in detail, we can separate the whole process into three phases:

In Phase 1, a Google form for collecting the consent with the information that are recorded in the process is explained. Consenting to the form, the participant will be able to move forward to the first set of questionnaires where the participants perspective towards authentication will be recorded in the Google form.

In Phase 2, the link to image-based authentication prototype that is hosted in Azure will be given to the participant. Utilizing that, participant can register and login in the prototype. The correct and incorrect click on the images is stored as a stamp along with user ID and time in the database to calculate the usability of the prototype.

In Phase 3, the participants will be able to click on a Google form for collecting the feedback of the prototype. Answering these questions based on their usage of the prototype will be an effective way to evaluate the whole prototype based on usability. The data collected from the Google form was insufficient as the graph lacked some specifics. As a result, the data were exported as .csv from the Google form and a more explicit graph with details was constructed for evaluation using matplotlib, a Python library.

The second evaluation was performed using the information stored during the participants login where correct/incorrect click login information was stored in the database. Using this a graph was plotted which claimed that participants selected fewer wrong points while logging in which adds a proof to the statement that was proved by the first evaluation.

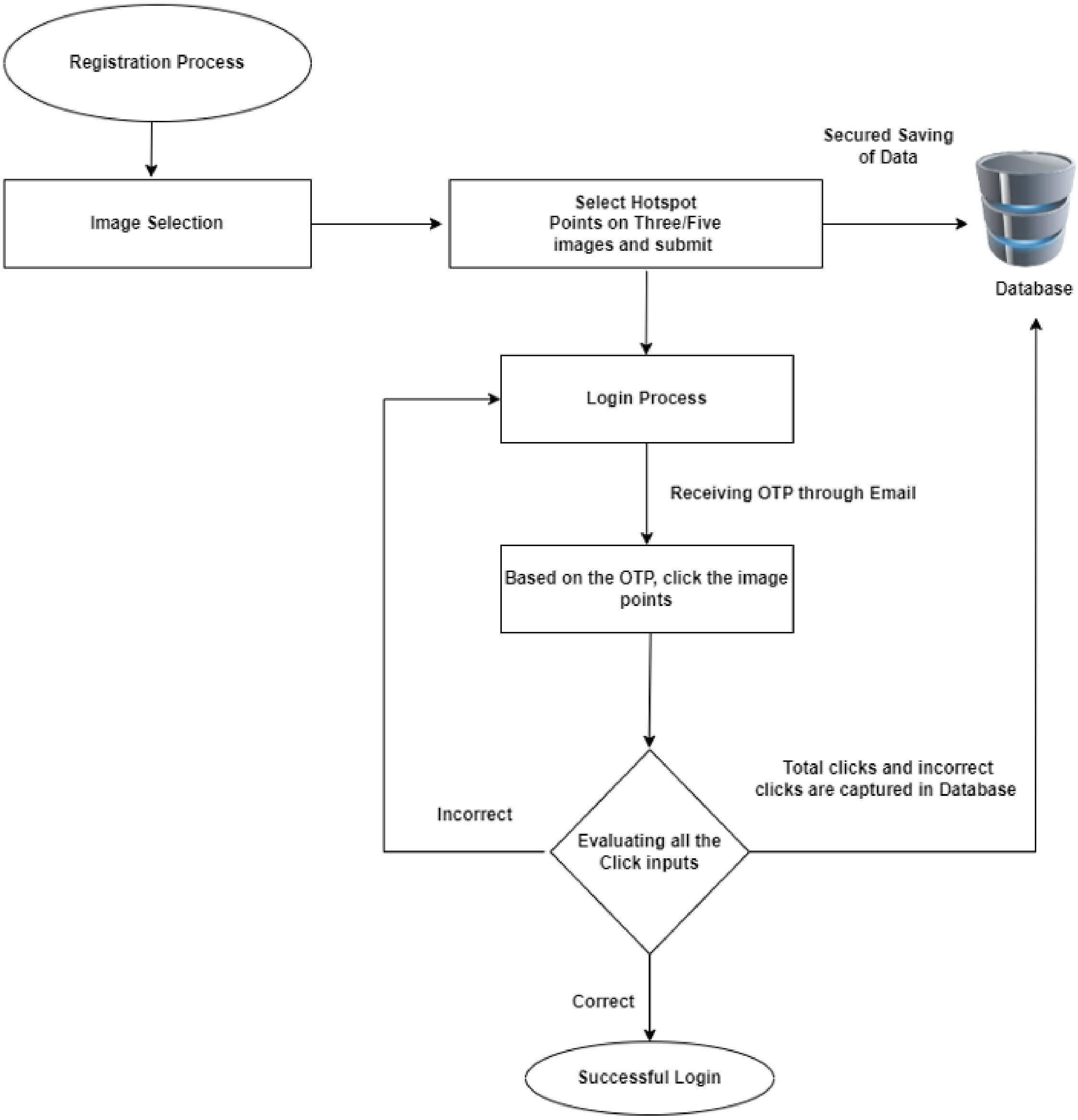
Registration Process
Image Selection
Select Hotspot Points on Three/Five images and submit
Secured Saving of Data
Database
Login Process
Receiving OTP through Email
Based on the OTP, click the image points
Incorrect
Evaluating all the Click inputs
Total clicks and incorrect clicks are captured in Database
Correct
Successful Login

Figure 2: Design flow of the prototype

4 Design Specification

4.1 Registration Phase:

Users must first finish a registration procedure before they use the application. Users are asked to provide certain mandatory information during the registration process.

4.2 Image selection phase:

The image selection phase is of two parts:

The first part requires the user to upload three of their personal choice of images into the prototype one after the other, followed by selecting a single point in each image to be used as a visual password. The second part is where three random images from the database will be provided for each registering user which will be not the same and the user is expected to select points on the image provided by the prototype. These data are then stored in the database.

4.3 Login phase:

In this phase the user can select what type of login he wants to proceed with that is with the M1(Username Password) or M2 (using Predefined images) or M3(using user uploaded images). When the user selects M1 they will be redirected to a page where they can login using traditional text-based password. When the user selects M2 or M3, they are required to input their Email id which will trigger a binary three-digit code to their email, based on the code (1 signifies correct point and 0 signifies wrong point) the user is expected to click the point on the image.

4.4 Background Information stored:

Here two background information are stored in the database:

- The time that was taken to complete the authentication/Login each time is displayed after the login.
- A time stamp of the correct and incorrect click is stored in the database as a separate new entry for each login.

If the user clicks on the logically correct point, a stamp with the time and id referencing correct will be added to the database, whereas if the user clicks on an incorrect point, a stamp with the time and id referencing incorrect will be entered in the database for each login. With the total number of logins tries that can be taken from adding both the correct and incorrect entries a graph will be plotted which can be used for evaluation of the model

5 Implementation

The proposed authentication method is intended to strengthen the system against a variety of cyberthreats by combining Persuasive Cued Click Points (PCCP) with an extra degree of security via email input for every image. Using Cued Click points, users can generate a password-protected visual representation of themselves by selecting specified locations on an image. This novel method improves security by giving the authentication procedure a visual and customised component. The model is implemented with JavaScript, Microsoft SQL Server and .NET, combining the dynamic and interactive characteristics provided by JavaScript with the strong capabilities of the.NET framework. The integration of email as an additional layer of security is a strategic measure to bolster the authentication process. The web prototype is hosted on the Azure platform, and Microsoft SQL Server Management Studio 19 was utilized to visualize and manage the associated database
When a user logs in the M2 or M3, the user is asked an email id to which the system triggers the SMTP (Simple Mail Transfer Protocol) protocol to send an email prompt. Based on the binary otp, the points of the image must be selected. This email contains a binary code (1 signifies correct point and 0 signifies wrong point) the user is expected to click the point on the images.

6 Evaluation

Based on the questions asked to the participants after using the prototype the following evaluations can be done.

Used visual aids such as graphs, charts, plots and so on to show the results.

6.1 Quantitative Data Analysis from Survey:

6.1.1 Case Study 1:

A total of 28 people took part in a survey and the following response were recorded after using the prototype:

What do you consider the most appealing aspect of image-based authentication?

After using the prototype, 67.9% of respondents found the three features of the offered image-based authentication PCCP—ease of use, personalization, and visual memorability—to be appealing. When compared to remembering a complex password with the recommended guidelines, trying to recall the points in this image-based authentication is comparatively simple. This could remove the need for password managers because there would be no need to write down or attempt to share passwords. The rationale behind personalization is that users were able to remember the points and log in accurately without selecting the wrong points because they chose their own pictures and the points that corresponded with those pictures. This assertion is supported by the fact that the wrong point selection was also observed. When compared to complicated text-based passwords, it is relatively easy to recall specific details from an image because visual memorability makes use of the brain's cognitive ability. This question reveals that the participants were more comfortable with the provided model based on the responses.

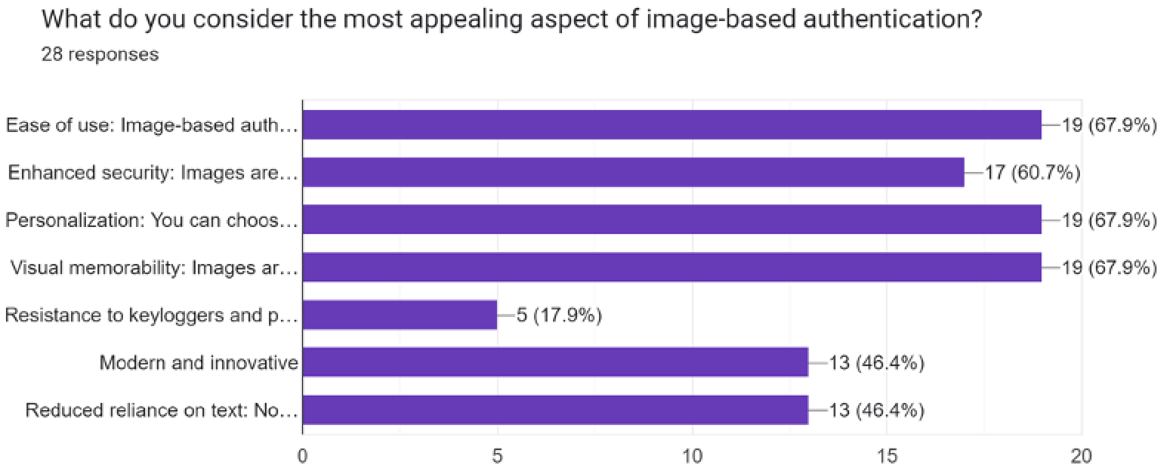

Figure 3: Case Study 1

6.1.2 Case Study 2:

When participants were asked to rate in “terms of password memorability, which method is preferable: the proposed image-based authentication model or traditional text-based password” the model indicated that the majority agreed as shown in the Figure 4.

(n=28, mode =4, mean = 3.857).

Therefore, this indicates that majority of the participants agreed that the proposed image-based authentication model is comparatively preferable than traditional text-based password in terms of memorability.

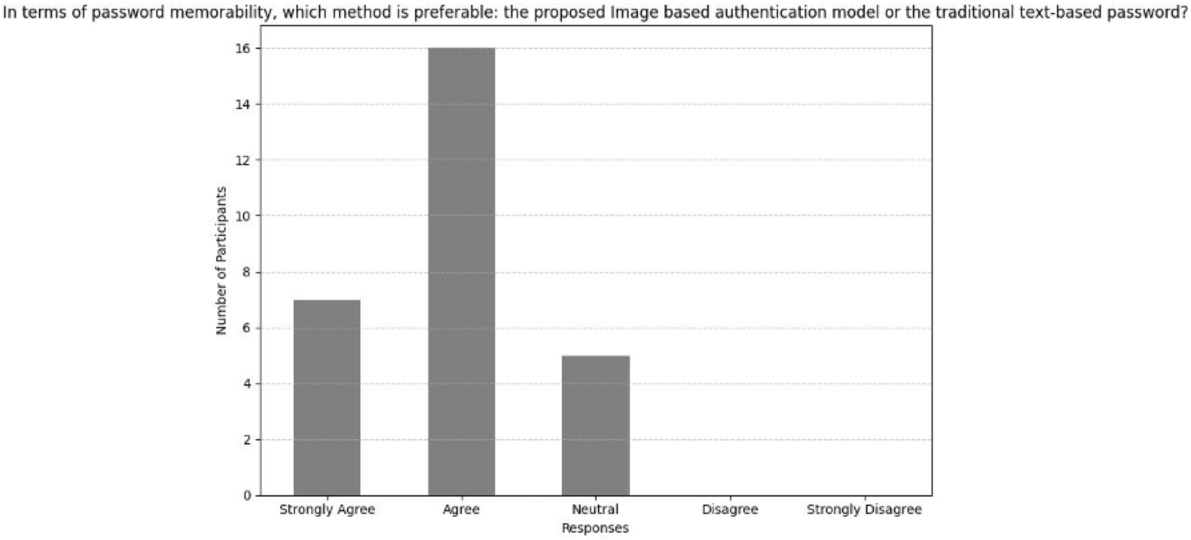

Figure 4: Case Study 2

6.1.3 Case Study 3:

When participants were asked “ Do you prefer to use PCCP as shown in the prototype over the traditional password-based mechanism ” the model indicated that the majority preferred to use PCCP with email over traditional text-based password as shown in the Figure 5. *(n=28, mean = 3.92, mode = 4)*

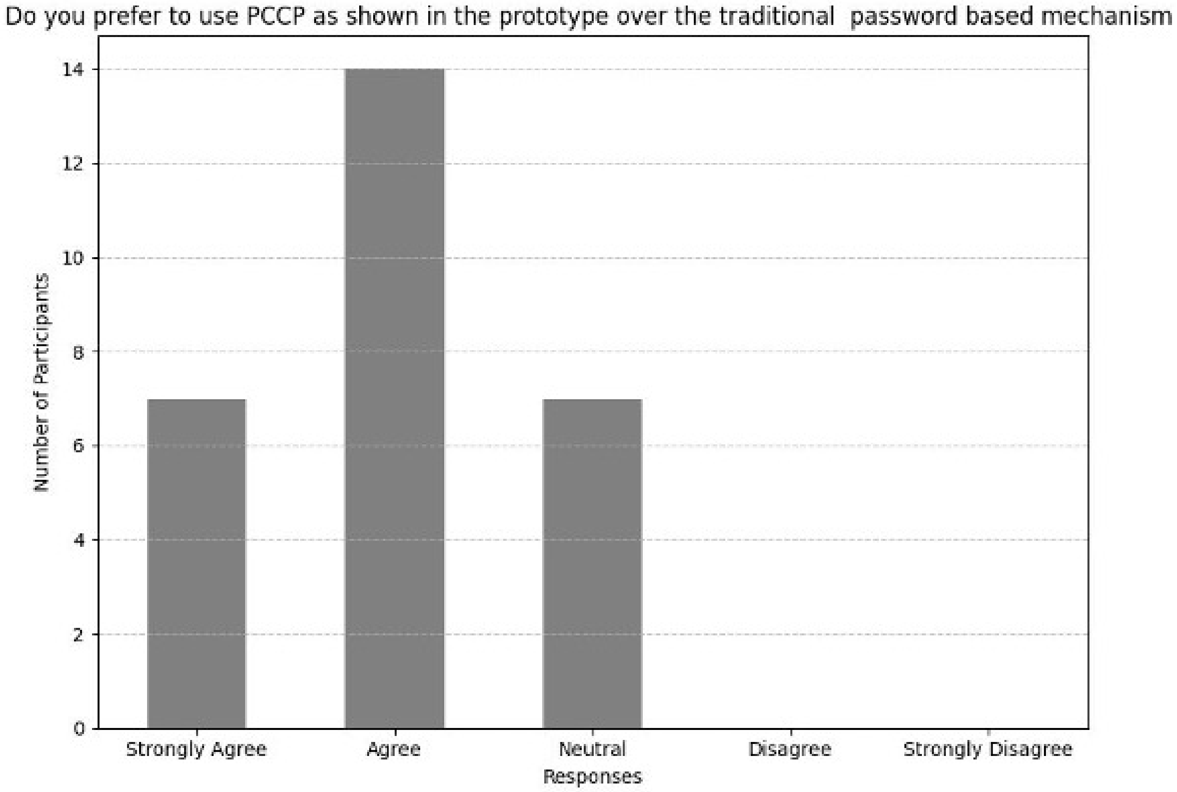

Figure 5: Case Study 3

6.1.4 Case Study 4:

When participants were asked “Would you be comfortable in using an image authentication method for an application or website” the model indicated that majority agreed as shown in the Figure 6. *(n=28, mean=4.14, mode =4).*

This reveals that based on the above feedback and the related study done by Chiasson et al. (2011) the usability and security perspective of the application is good and ease of use for the participant.

6.2 Quantitative Data Analysis based on Background Data:

In the Prototype, a dynamic and informative metric that provides a full perspective of user interactions and system performance is the Click Point Match Status Over Time with Accuracy for images that are selected during login. The system generates a comprehensive timeline of authentication attempts by monitoring the Click Point Match Status across login dates and linking it to User IDs. The ability to recognise patterns and trends

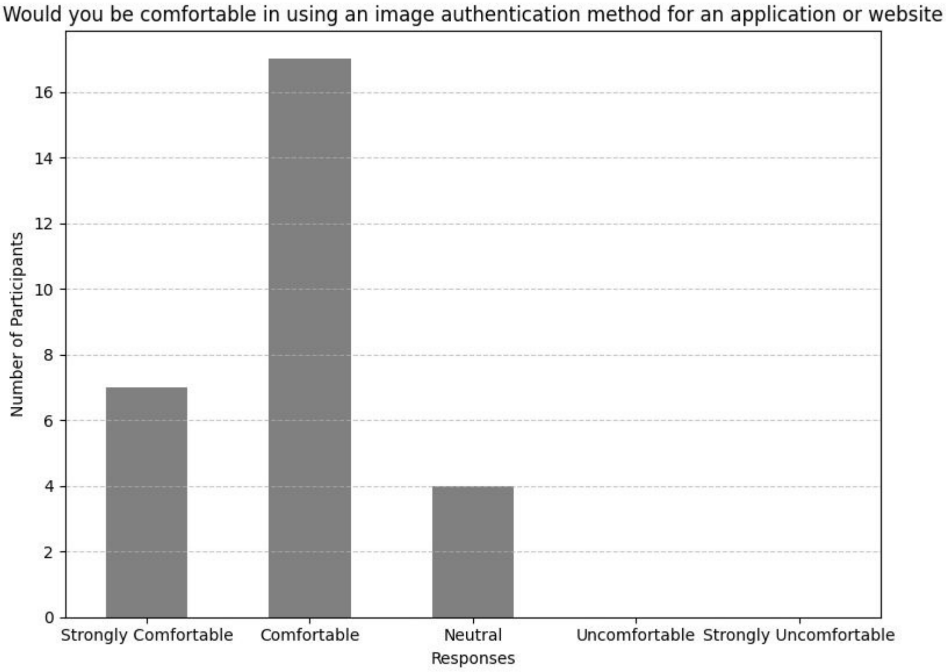

Figure 6: Case Study 4

through time analysis facilitates the discovery of any abnormalities or potential security risks. The selected Click Point Match Status for Predefined Images is shown in Figure 7.

The evaluation of Predefined Image Accuracy involves linking User IDs to the quantity of clicks performed by individual users during login attempts. This metric provides a detailed insight of the participants comfortability and the overall dependability of the visual password system by quantifying the success rate in aligning specific spots on predetermined images. The time and the performance of each individual user are combined to allow the system to adjust and improve based on trends that are noticed.

The total number of login attempts is reflected in the number of clicks field, which provides information on the user's involvement. The accuracy ratio, which is determined by dividing the total number of clicks into correct and incorrect ones, measures each user's success rate and highlights how successful the visual password system is. Frequent examination of these factors guarantees a balanced strategy, fostering both user-friendly interaction and strong security in the Cued Click Prototype's authentication procedure. The accuracy ratio for each user's click point match of user image is displayed in Figure 8.

6.3 Discussion

The study in its entirety offers a thorough investigation of the viability, security, and user acceptability susceptible of image-based authentication. It includes the registration, login, and user feedback components inside the Cued Click Prototype. The study draws several major conclusions and implications. To begin, we can see from Case Study 1 that the majority of participants chose the image authentication prototype's feedback as ease of use, personalization, and visual memorability. This indicates that the participants believe remembering a strong password is comparably hard when compared to remembering

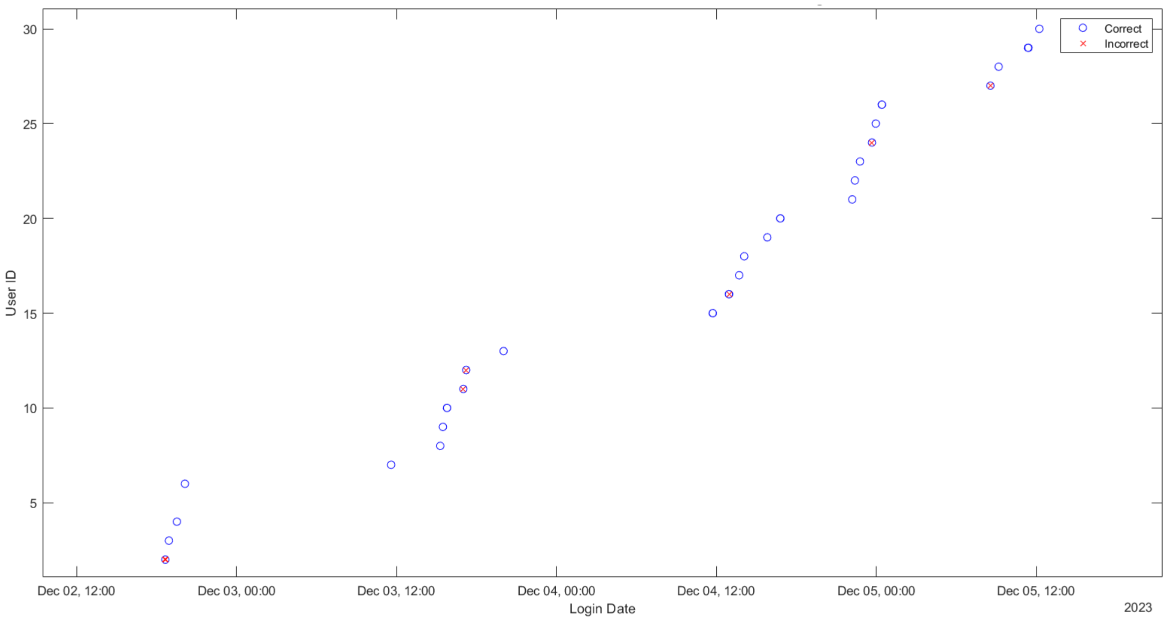

Figure 7: Click Point Match Status Over Time

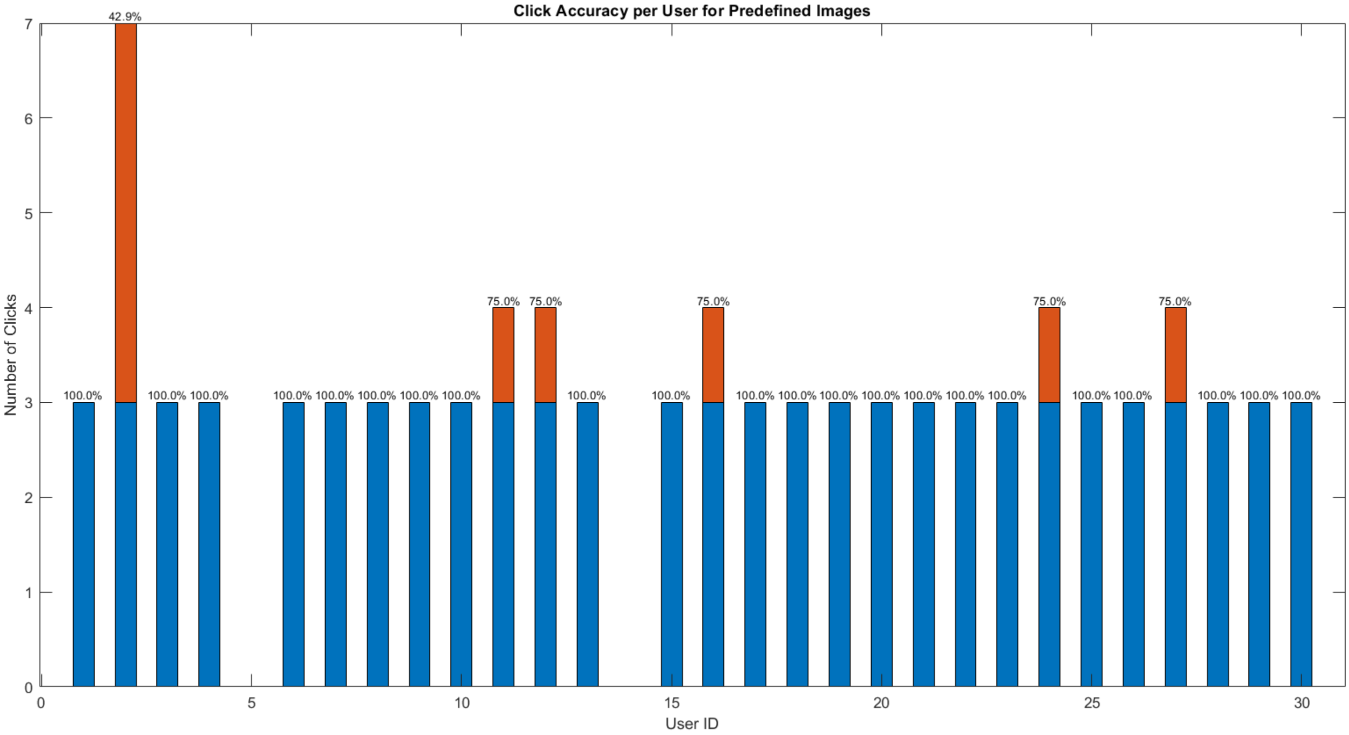

Figure 8: Accuracy Ratio for Each Images of Click Point Match

certain points of an image they upload. This gives a positive uplift that the usability of the proposed image-based authentication prototype is comfortable for the users when comparing it with text-based authentication.

Case studies 2 and 3 show that participants find the proposed image-based authentication prototype more comfortable than text-based authentication because the selected points on the image are easy to remember, supporting the previous case study's conclusion. Based on case study 4, we may assume that the majority of participants felt comfortable using the proposed image-based authentication methodology for a website or application. This indicates that the prototype is preferred by the survey participants. Based on the background data captured during the login phase the following graph Figure 7 was plotted which signifies the correct/incorrect login attempts that were made by the participants.

Since PCCP has multiple images than CCPs and Pass Points, hotspot and click point clustering is less vulnerable. The presence of several images makes phishing impossible. With a graphical password, guessing attacks are less likely to be successful Chiasson et al. (2011). By selecting inputs based on a binary OTP, the system strengthens its defences against hotspots and majority of the attacks listed.

7 Conclusion and Future Work

The effect of combining Persuasive Cued Click Points (PCCP) with Email Authentication on improving user experience and security in web authentication was studied. According to the survey results, participants were comfortable using the PCCP through Email authentication prototype, and the majority of participants were comfortable using the proposed image authentication model in place of traditional text-based authentication. This adds a proof that PCCP and email verification when integrated works smoothly and yields security and usability for the authentication process which overcomes shoulder surfing and provides utmost security without any compromise in memorability, security and user experience.

Additional encryption algorithms can be used to encrypt the images stored in the database, increasing the overall model's security. Integrating an AI model that generates images with more details for more clickable points will significantly improve the security of this method. Machine learning algorithms can be used to learn the image's strong and weak points and can be added to the PCCP method to provide a critical review based on the selected point, drastically reducing the success rate of cyber-attacks in this method.

References

Abbas, S. F. and Jawad, L. M. (2023). Pass point selection of automatic graphical password authentication technique based on histogram method, *Iraqi Journal of Information and Communication Technology* **6**(1): 28–39.

Ameen, J. N., Mohamed, J. J. and Begam, N. N. (n.d.). Efficient authentication scheme using pccp.

Brostoff, S. and Sasse, M. A. (2000). Are passfaces more usable than passwords? a field trial investigation, *People and computers XIV—usability or else! Proceedings of HCI 2000*, Springer, pp. 405–424.

Chiasson, S., Stobert, E., Forget, A., Biddle, R. and Van Oorschot, P. C. (2011). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism, *IEEE transactions on dependable and secure computing* **9**(2): 222–235.

Ghiyamipour, F. (2021). Secure graphical password based on cued click points using fuzzy logic, *Security and Privacy* **4**(2): e140.

J, K. (2020 Jul 8). Why enterprises should use certificate-based authentication as access control. Accessed on December 01, 2023.
URL: *https://swoopnow.com/website-authentication/.* -

Kathole, A. B., Jaiswal, M. A., Chaudhari, M. S. and Kapile, M. A. (n.d.). To avoid shoulder surfing using graphical password.

Kenneth, M. O. and Olujuwon, S. M. (2021). Web application authentication using visual cryptography and cued clicked point recall-based graphical password, *Journal of Computer Science Research* **3**(3): 29–41.

Khan, A. and Chefranov, A. G. (2020). A captcha-based graphical password with strong password space and usability study, *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, IEEE, pp. 1–6.

Moraskar, V., Jaikalyani, S., Saiyyed, M., Gurnani, J. and Pendke, K. (2014). Cued click point technique for graphical password authentication, *International Journal Of Computer Science And Mobile Computing* **3**(1): 166–172.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018). Multi-factor authentication: A survey, *Cryptography* **2**(1): 1.

Saha, H., Saha, G. C., Roshidul, H., Islsam, Z. et al. (2019). User authentication through cued click points based graphical password, *American Journal of Agricultural Science, Engineering, and Technology* **3**(1): 10–24.

Sunil, S. S., Prakash, D. and Shivaji, Y. R. (2014). Cued click points: Graphical password authentication technique for security, *IJCSIT) International Journal of ComputerScience and Information Technologies* **5**(2).