**Randomized Point Selection in Graphical Password Authentication: A Secure Approach for Educational Systems**

**Adegbola Ismail Adelabu**

Department of Computer Science, Oyo State College of Education, Lanlate

[adegbolaia@oyscoel.edu.ng](mailto:adegbolaia@oyscoel.edu.ng)

ABSTRACT The rise in cyber threats has really underscored the importance of having secure yet user-friendly ways to authenticate ourselves online. This study presents an innovative graphical authentication system that uses randomized point selection, which we’ve named the Encrypted Cued Click Point System (ECCPS). With this system, users can upload up to five personal images, each featuring three randomly generated points. When it comes time to authenticate, users need to pick one correct point from each image, creating a unique combination for secure access. By randomizing the point selection, ECCPS helps reduce the risks of shoulder-surfing and guessing attacks. We implemented the system on an academic result management platform and put it to the test with 50 students. We looked at various metrics, including how often users successfully authenticated, error rates, the time it took to authenticate, and overall user satisfaction to evaluate both usability and security. The results show that ECCPS strikes a great balance between strong security and user-friendliness, with over 90% of participants managing to authenticate within three tries and an average authentication time of 20 seconds. Participants provided positive feedback, pointing out the system's potential for wider use in handling sensitive information. This paper dives into the design, implementation, and evaluation of ECCPS, highlighting how it contributes to the evolution of graphical password systems.

KEYWORD: Graphical Passwords, Randomized Point Selection, User Authentication, Usability, Educational Systems, Information Security, Human-Computer Interaction

1. INTRODUCTION

In today’s digital age, authentication is a critical component of information security and it provide the foundation for protecting sensitive data and systems (Ugli, 2024). Educational sector demand for system authentication with a robust security and ease of use because of the heavy reliance on online to carry out virtually all educational activities. Traditional alphanumeric passwords system is the major authentication system in online services and information system in Nigeria. Despite its uniqueness and ubiquity, it is prone to vulnerabilities due to conflicting requirement; security and ease of use (Ezugwu et al., 2023). The user finds it very difficult to meet both of these requirements. From a security viewpoint, the ideal password is a string of eight or more random characters, including digits, letters with a mixture of upper and lower case, and special characters. This can only be learned by rote in traditional text-based password system. The user out of ease of use selects weak password and for memorability and decreasing the memory burden of recall write the password down and reuse the same password across multiple platforms thus making them susceptible to phishing, shoulder surfing and brute force attack (Yıldırım & Mackie, 2019). This major problem has spring up alternative authentication system like graphical password system as a potential solution authentication system.

Katsini et al., (2018) stated that graphical password popularity is leverage on the cognitive and psychology of human ability to remember images than text. The research has showed that human being can recall images than text and this has given rise to image password system. Various graphical password scheme like click points, image recognition and grid-based scheme have emerged and in use, but most of them are either suffering from ease of use, involve complex process in implementation and usage or not resistant to attack coming from observation and shoulder surfing (Fernando, Dissanayake, Dushmantha, Liyanage, & Karunatilake, 2023).

This study presents a novel graphical password authentication named Encrypted Cued Click Point System (ECCPS). It is a graphical authentication mechanism that is designed to improve system security without compromising ease of use. The system introduces randomized point selection on user-uploaded images upon registration which make authentication process dynamic and robust. The researcher evaluates the usability, security and real-life application by deploying ECCPS on a departmental academic record management system. The ECCPS builds upon the philosophy of cued click point model by introducing a layer of randomization to enhance security. It requires users to interact with dynamically generated points on personal images upon registration, ECCPS reduces predictability and strengthens resistance against common attack vectors. It also addresses common graphical password vulnerabilities and ensures a dynamic and secure authentication experience This study situates ECCPS within the broader context of graphical authentication research, aiming to address gaps in usability and security while providing empirical evidence through its deployment and evaluation.

Authentication plays a crucial role in keeping our information secure, making sure that only the right people can access sensitive data and systems. Traditional methods, like alphanumeric passwords, often fall short because users tend to pick weak or easily guessable passwords. On top of that, the increasing sophistication of cyberattacks has exposed the weaknesses of these methods when it comes to providing solid security. To tackle these issues, graphical password systems have emerged as a promising alternative. These systems tap into our natural ability to remember and recognize images or visual elements, which is usually a lot easier than trying to recall a string of letters and numbers. There are several interesting types of graphical password models that have been developed, such as:

1. Recognition-Based Systems: In these, users pick out images they’ve previously selected from a set.
2. Recall-Based Systems: Here, users draw or recreate a specific pattern.
3. Cued Recall Systems: This type requires users to select certain spots on an image to use as their password.

Safder (2024) is of the opinion that the most graphical model, serving as the foundation of ECCPS, has shown considerable promise in improving memorability while ensuring security. However, current implementations often lack mechanisms to prevent observation attacks or struggle to scale effectively to meet the diverse needs of users as user may need to remember complex graphical password. ECCPS enhances this model by integrating randomization and encryption, offering a more secure and user-friendly solution. Numerous studies have examined the design, usability, and security of graphical password systems. A number of studies have looked into how graphical password systems are designed, how user-friendly they are, and their security features. Suo, Zhu, and Owen (2005) provided a detailed critique of the traditional alphanumeric password method, which relies on usernames and passwords. They also gave an overview of graphical password schemes, pointing out both their advantages and disadvantages. Their analysis emphasized the need to create systems that strike a good balance between being easy to use and being tough against attacks such as shoulder surfing and brute force.

Biddle, Chiasson, and van Oorschot (2012) carried out a thorough survey on graphical passwords, breaking them down into three categories: recognition, recall, and cued recall systems. They discovered that cued recall systems hold the most potential because they strike a good balance between being memorable and secure. However, they also pointed out that there’s a pressing need for new ideas to improve scalability and resistance to attacks. Thorpe and van Oorschot (2007) took a close look at the security of click-based graphical passwords and pointed out some weaknesses, particularly when it comes to hotspot attacks. In these attacks, hackers take advantage of the areas in an image that users tend to click on the most. To tackle this issue, ECCPS brings in a bit of randomness, which helps make it harder to guess where users are likely to click. A study conducted by Chiasson et al. (2009) looked into how effective cued click points are and suggested some design tweaks to make the user experience better. Taking these findings into account, ECCPS now allows users to upload their own images, which adds a personal touch and makes things more memorable, all while keeping security intact with a randomized point selection process.

1. METHODOLOGY

The Encrypted Cued Click Point System (ECCPS) is built on the core ideas of usability, security, and scalability. Its architecture is crafted to provide a smooth user experience while also protecting against typical attack methods.

Registration

New User

Image upload

Point Generation on Image based on randomization

Point Selection

Selected points

Stored

**Figure 1:** Framework of the Encrypted Cued Click Point

**Key Features of ECCPS**

1. Image Personalization: Users have the option to upload up to five personal images, which helps make the experience more familiar and memorable.
2. Randomized Point Selection: Each time you authenticate, three points are randomly generated on each image, making it less predictable.
3. Encryption: The chosen points are encrypted and stored securely to keep unauthorized access at bay.
4. Dynamic Interaction: During authentication, users need to select one correct point from each image, resulting in a unique and engaging password experience.

The Encrypted Cued Click Point System (ECCPS) was created to provide a secure way for users to authenticate their graphical passwords in educational settings. To get started, users need to upload up to five images. Each of these images is then linked to three clickable points, which are generated through a randomization algorithm. This clever approach guarantees that no two users will have the same set of clickable points, adding an extra layer of security

**User Registration**

**Step 1:** Users upload up to five personal images (e.g., personal photographs or images of significant landmarks).

**Step 2:** The system applies a randomization algorithm to select three points on each image, ensuring that the points are non-repetitive.

**Step 3:** Users are asked to select one of the three points on each image, and their choices are recorded as part of their graphical password.

**Step 4:** Selected points are encrypted and stored securely in the database.

**Authentication Process**

**Step 1:** During login, the system displays the uploaded images with randomized points and the users must select the predetermined points (randomly assigned during registration).

**Step 2:** The system compares the user’s selection with the stored selections to authenticate the individual. The randomization of points ensures that even if an image is compromised, the likelihood of guessing the correct point reduces significantly.

**Step 3:** The system validates the selections against the encrypted data.

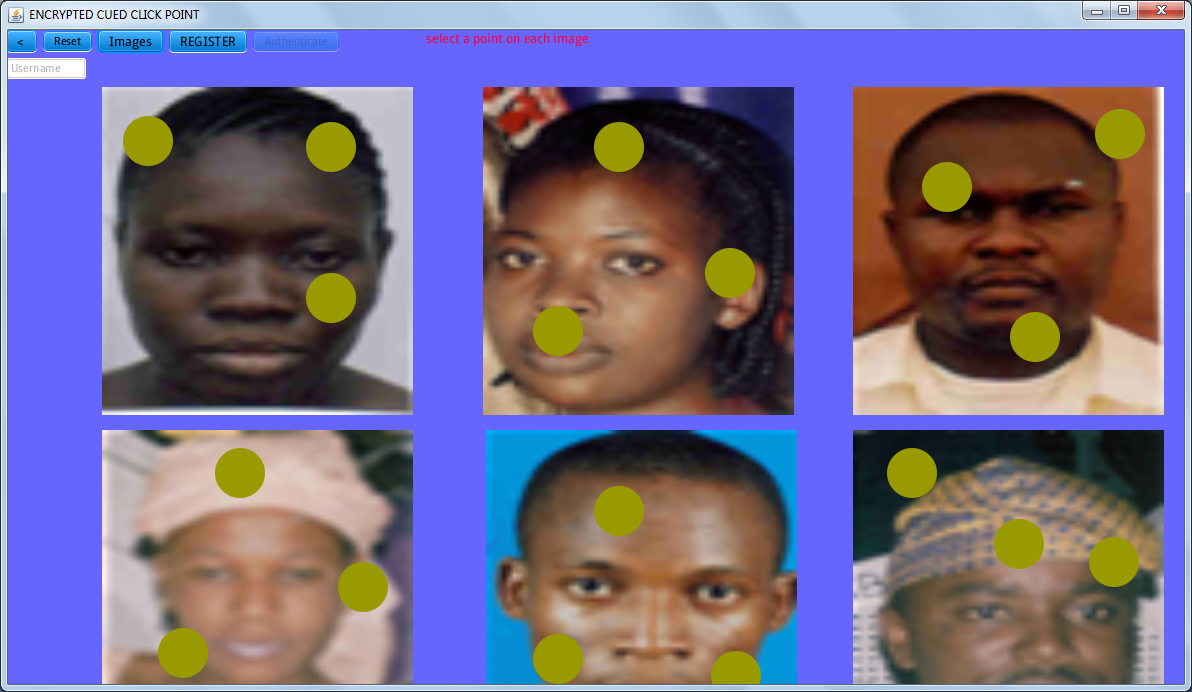
**Security Measures**

* 1. **Encryption**: Ensures the confidentiality of stored authentication data.
  2. **Randomization**: Prevents attackers from exploiting predictable patterns.
  3. **Session Logging**: Tracks authentication attempts for monitoring and analysis.

**Evaluation Metrics**

* 1. **Usability**: This was measured through success rates, time to authenticate, and user feedback.
  2. **Security**: Assessed based on error rates and resistance to attacks such as shoulder surfing and brute force.

The figure below shows the interface of the encrypted graphical password with randomized point generated on uploaded images for registration.



**Figure 2:** Randomized Point Generated on Uploaded Images

**Use-Case Description of ECCP**

A use case in software development is basically a way to illustrate how users engage with a system to achieve a specific goal. It outlines the steps or scenarios involved in completing a task or process. Use cases are incredibly useful because they help clarify what the system needs to do and how it should behave from the user's perspective. In the world of software development, they play a crucial role in modeling and communicating functional requirements. Typically, a use case will feature actors, actions, and the system's responses to those actions. Below, you'll find a few examples of system use cases.

**Table 1:** Flow of Events for Login Process

|  |  |
| --- | --- |
| Use-Case | Description |
| Login | An existing user must login to interact with the system:  Actor/s: User  Pre-Condition:  A User has Registered  Flow of events:  1. The USER clicks the EXISTING USER button on the Home Page.  2. The system displays the Log-in Page.  3. The USER enters his/her username.  4. The USER clicks LOGIN.  5. The system validates the username information against the User Information Table in the database.  6. Username exists; the system uploads the login images.  8. The USER enters his/her password by clicking on a point per sequence of images.  9. The USER clicks the AUTHENTICATION button.  10. The system validates the click point selected against the  Click points in the database.  11. USER is an authorised user; the system displays a message  “Authenticated!! Login Successfully!!” to the USER.  Post-condition:  The USER has been authorised to use the system. |
|  | Alternate flow of event:  1. The USER clicks the EXISTING USER button on the Home Page.  2. The system displays the Log-in Page.  3. The USER enters his/her username.  4. The USER clicks the LOGIN button.  5. The system validates the username information against the User Information Table in the database.  6. USER does not exist; the system displays a pop-up message  “Invalid user” to inform the USER.  Post-condition:  The USER has not been authorised to use the system |
|  | Alternate flow of event:  1. The USER clicks the EXISTING USER button on the Home Page.  2. The system displays the Log-in Page.  3. The USER enters his/her username.  4. The USER presses the CANCEL button.  5. The system stops the transaction.  Post-condition:  No changes are made to the USER account. |
|  | Alternate flow of event:  1. The USER clicks the EXISTING USER button on the Home Page.  2. The system displays the Log-in Page.  3. The USER enters his/her username.  4. The USER clicks LOGIN.  5. The system validates the username information against the User Information Table in the database.  6. Username exists; the system uploads the login images.  7. The USER enters his/her password by clicking on a point per sequence of images but leave a point.  8. The USER clicks the AUTHENTICATION button.  9. The system validates the click point selected against the  Click points in the database.  10. USER is not an authorised user; the system displays a message “LOGIN PROBLEM Select all points”  Post-condition:  The USER is not authorised to use the system. |

**Table 2:** Flow of Events for Register Process

|  |  |
| --- | --- |
| Use-Case | Description |
| Register | A new USER needs to be registered into the system before Using the system  Actor/s: USER  Pre-condition: USER has not been registered.  Flow of events:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all of the required information including the username.  4. The USER clicks the NEXT button.  5. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  6. The images are correct system display the images on the screen.  7. The USER is asked to select a point per image as password.  8. The USER click on the REGISTER button to complete the registration.  9. The system shows the selected point for mastering and review.  10. The USER clicks the CONFIRM button.  11. The system updates account information in the User Information and  PASSWORD tables in the database.  12. The system returns the USER to the Log-in Page.  Post-condition:  The new USER has been registered. The User Information and PASSWORD tables are updated. |
|  | Alternate flow of event:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all of the required information including the username.  4. The USER clicks the NEXT button.  5. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  6. The images are not correct system display a message “Image dimension or format not correct”.  7. The USER is asked to upload correct images.  Post-condition:  The new USER has not been registered. The User Information and PASSWORD tables have not been are updated are updated. |

|  |  |
| --- | --- |
|  | Alternate flow of event:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all of the required information including the username.  4. The USER clicks the NEXT button.  5. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  6. The images are not correct system display a message “Image dimension or format not correct”.  7. The USER is asked to upload correct images.  8. The USER re upload correct image and the system display the images on the screen.  9The USER is asked to select a point per image as password.  10. The USER click on the REGISTER button to complete the registration.  11. The system shows the selected point for mastering and review.  12. The USER clicks the CONFIRM button.  13. The system updates account information in the User Information and  PASSWORD tables in the database.  14. The system returns the USER to the Log-in Page.  Post-condition:  The new USER has been registered. The User Information and PASSWORD tables are updated |

|  |  |
| --- | --- |
|  | Alternate flow of event:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all a user name that has already been used by another person the system display a message “Username exist” and asks the user to enter another username.  4. USER re-enter another username.  5. The USER clicks the NEXT button.  6. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  7. The images are not correct system display a message “Image dimension or format not correct”.  8. The USER is asked to upload correct images.  9. The USER re upload correct image and the system display the images on the screen.  10The USER is asked to select a point per image as password.  11. The USER click on the REGISTER button to complete the registration.  12. The system shows the selected point for mastering and review.  13. The USER clicks the CONFIRM button.  14. The system updates account information in the User Information and  PASSWORD tables in the database.  15. The system returns the USER to the Log-in Page.  Post-condition:  The new USER has been registered. The User Information and PASSWORD tables are updated |

|  |  |
| --- | --- |
|  | Alternate flow of event:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all a user name that has already been used by another person the system display a message “ Username exist” and ask the user to enter another username.  4. USER re-enter another username.  5. The USER clicks the NEXT button.  6. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  7. The images are not correct system display a message “Image dimension or format not correct”.  8. The USER is asked to upload correct images.  9. The USER re upload correct image and the system display the images on the screen.  10The USER is asked to select a point per image as password.  11. The USER click on the REGISTER button to complete the registration.  12. The system shows the selected point for mastering and review.  13. The USER change the selected click points on the image  14. The USER clicks the CONFIRM button.  15. The system updates account information in the User Information and  PASSWORD tables in the database.  16. The system returns the USER to the Log-in Page.  Post-condition:  The new USER has been registered. The User Information and PASSWORD tables are updated |

|  |  |
| --- | --- |
|  | Alternate flow of event:  1. The USER clicks the NEW USER button on the Home Page.  2. The system displays the Registration Page.  3. The USER enters all a user name that has already been used by another person the system display a message “ Username exist” and ask the user to enter another username.  4. USER re-enter another username.  5. The USER clicks the NEXT button.  6. The USER is asked to upload 6 images of dimension 250x331 and of JPEG format.  7. The images are not correct system display a message “Image dimension or format not correct”.  8. The USER is asked to upload correct images.  9. The USER re upload correct image and the system display the images on the screen.  10The USER is asked to select a point per image as password.  11. The USER click on the REGISTER button to complete the registration.  12. The system shows the selected point for mastering and review.  13. The USER change the Username  14. The USER clicks the CONFIRM button.  15. The system updates account information in the User Information and  PASSWORD tables in the database.  16. The system returns the USER to the Log-in Page.  Post-condition:  The new USER has been registered. The User Information and PASSWORD tables are updated |

**User Experimental Study and Feedback**

A usability study was conducted with 50 students from the Department of Computer Science at Oyo State College of Education, Lanlate. Participants were required to register, authenticate, and provide feedback on the system's ease of use, perceived security, and satisfaction.

1. RESULTS AND DISCUSSIONS

User Registration and Authentication Performance

**Table 3: Summary of Experimental Metrics (n = 50)**

|  |  |
| --- | --- |
| Metric | Value |
| Average Registration Time | 5.2 minutes |
| Average Authentication Time | 20 seconds |
| Success Rate (First Attempt) | 96% (48 out of 50) |
| Errors Due to Forgetfulness | 4% ( 2 users) |

The average registration time (Mean = Sum of Reg Time / 50): This is simply calculated as the total time taken for all users to register, divided by 50. i.e Sum of all individual registration times divided by 50. Therefore, all users average 5.2 minutes to register stating from the image upload, point selection to final submission.

**Authentication time:** This is the average duration it took for users to log in on their first try. Each individual user average 20 seconds to select their point for authentication. The success rate (Success Count = Count of Yes in Login Success): This is the number of users who logged in successfully on their first attempt, divided by the total number of users, and then multiplying by 100. So, 48 out of 50 users succeeded, therefore, (48/50) × 100 = 96%. Error rate (Error Count = Count of Yes in Error column): This is the number of users who clicked on the wrong points during login because of memory lapses. So, 2 out of 50 users failed the login process, therefore (2/50) x 100 = 4%

**Figure 3:** The Visual Authentication Performance

**Figure 4:** The Login Output of the participants

The system showed impressive registration success, with 98% of users able to upload images and select points without any problems. On average, it took them about 5.2 minutes to complete the registration process. The authentication success rates were also noteworthy, as 96% of participants managed to authenticate on their first try, taking around 20 seconds each to select their point for authentication.

**Table 4:**

**Security Evaluation**

|  |  |  |  |
| --- | --- | --- | --- |
| Attack Type | Attempts | Successful Breaches | Comments |
| Brute-force | 100 | 0 | High password entropy |
| Shoulder Surfing | 10 | 0 | Points randomized |

A group of ten students was chosen to keep an eye on the user during the registration process, and they were later asked to try accessing the system with 100 authentication attempts. Unfortunately, all the students were unable to get through the authentication process due to the randomization involved. This showed that the system is quite robust against brute-force attacks. The way the points are randomized also greatly expanded the password space (5 images × 3 points = 15 possible selections for each user). Even if an attacker had access to all the images, the odds of picking the correct points in the right order were extremely low, making it tough to breach the system.

**Usability Evaluation**

To evaluate how user-friendly the proposed graphical password authentication system is, we had 50 students fill out the System Usability Scale (SUS) after they completed the registration and authentication tasks. The SUS consists of ten standardized statements that participants rate on a five-point Likert scale, mixing positive and negative sentiments to get a sense of their experience and satisfaction. We then adjusted each response following the standard SUS scoring method, which gave us individual usability scores that range from 0 to 100.

**SUS Results**

Out of the 50 participants:

1. The average SUS score was 82.1
2. The standard deviation was 6.5
3. 78% of participants scored above 80, indicating high usability
4. No participant scored below 65, suggesting an overall positive user experience

According to (Brooke, 1996), SUS scores above 68 are considered above average, and those above 80 signify excellent usability. The high mean SUS score confirms that users found the system easy to learn, straightforward to use, and efficient in achieving authentication tasks.

**User Feedback and Observations**

The qualitative feedback from participants really backed up the numbers we found:

1. The majority of users loved the intuitive image-based approach and thought the randomized point selection feature was both fresh and effective.
2. A handful of participants were a bit unsure about the authentication process at first, but that uncertainty faded away with a little guidance and some practice.

The ECCPS framework is crafted to strike a balance between the often-conflicting needs of security and usability, making it a flexible solution for various application scenarios. This study seeks to confirm its effectiveness by putting it to the test in real-world deployments and user trials, ultimately providing solid evidence of its ability to overcome the shortcomings of current graphical authentication systems.

**Enhanced Security through Randomization**

The standout feature of the ECCPS system is its clever use of randomized point selection. This approach greatly boosts security by making it tough for attackers to guess or predict password points from the images they see. By randomizing the points, we eliminate any fixed patterns, which helps lower the chances of shoulder-surfing and other types of observation-based attacks. Improved Usability. The visual aspect of the authentication process really made the system more engaging and user-friendly compared to the old-school text-based password systems. Sure, first-time users might face a bit of a learning curve, but that was quickly sorted out after they completed the initial registration.

**Challenges and Limitations**

One of the limitations highlighted in the study was that users often had a hard time recalling the exact locations of the points on the images, particularly if they managed multiple accounts or frequently switched up their images. Offering users some hints or utilizing a smaller selection of images could really help lighten the cognitive load.

**Future Work**

In the future, we’ll see the system evolve to include multi-factor authentication. This means users will need to mix graphical passwords with other verification methods, like biometric checks or one-time passwords (OTPs). Plus, we’re making sure the system works seamlessly on mobile devices, keeping in mind how much people depend on their smartphones for accessing education.

**Implications for Educational Systems**

Using graphical password authentication in schools tackles a lot of security issues, particularly when it comes to safeguarding sensitive student information. Its flexibility and ease of use make it a great alternative to the usual password methods, providing better security for both administrators and users alike.

**REFERENCES**

1. Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (pp. 10-pp). IEEE.
2. Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 1-41.
3. Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., ... & Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*, e01743.
4. Ugli, Y. S. S. (2024). INFORMATION SECURITY AND ITS COMPONENTS. *International Journal of Advance Scientific Research*, *5*(12), 302-311.
5. Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, 741-759.
6. Katsini, C., Fidas, C., Raptis, G. E., Belk, M., Samaras, G., & Avouris, N. (2018, April). Influences of human cognition and visual behavior on password strength during picture password composition. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-14).
7. Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and opportunities in password management: a review of current solutions. *Sri Lanka Journal of Social Sciences and Humanities*, *3*(2).
8. Safder, W. (2024). Password Security, An Analysis of Authentication Methods.
9. Chiasson, S., Biddle, R., & Van Oorschot, P. C. (2007, July). A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 1-12).
10. Chiasson, S. (2009). *Usable authentication and click-based graphical passwords* (Doctoral dissertation, Carleton University).