M. Mohanedova *et al*, International Journal of Advances in Agricultural Science & Technology,
Vol.11 Issue.4, April 2024, pg. 106-113

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

A Multi-Layered Graphical Password Authentication Scheme to Resist Visual Hacking

Dr. Y. Jayababu [1] , Medapati Navya Sri [2], Peruri Madhuri Deepika [3], Penumala Niharika [4], Kandula Sri Ram [5], Shaik Babji [6] , [1]Professor , [2, 3, 4, 5, 6]B.tech Students Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India
Email: jayababu.y@pragati.ac.in

Abstract:

Password-based authentication is a popular way for ensuring computer application security and privacy. Nonetheless, the "weakest link" in the authentication process is believed to be user-chosen weak passwords and hazardous input techniques. People generally utilize mnemonic or brief passphrases instead of random alphanumeric characters. Because internet and mobile applications are widely available, users can access them from any location, at any time, using any device. While this simplicity is generally appreciated, it also increases the likelihood that credentials will be compromised through Visual Hacking. The assault tactics can include employing external recording equipment or watching the victim personally in order to obtain their login information. In response to this issue, our team created a graphical password-based authentication mechanism to combat the threat of Visual Hacking. The system's security mechanism is three-tiered, featuring password verification as well as colour and pattern matching features. This means that even with numerous camera-based hacking attempts, potential attackers would have a tough time determining or limiting the password. In addition, we created and tested a system prototype to determine its usability. According to our trial results, our system can survive Visual Hacking better than previous authentication systems while maintaining a high level of security and usability.

Keywords: Credential theft, Alphanumeric strings, Visual Hacking, Security, Graphical Authentication

I. Introduction

For decades, textual passwords have reigned supreme as the go-to authentication method, relying on a combination of numerals and upper and lower-case letters to fortify resistance against brute force attacks. Despite them prevalence, however, the degree of complexity required to render these passwords truly secure renders them notably arduous to memorize and recall. Consequently, users often succumb to the temptation of selecting passwords that are either too short or easily derived from the dictionary [7], as opposed to employing a random alphanumeric sequence. This troubling trend is exacerbated by the fact that individuals frequently employ the same login credentials across multiple accounts, thus creating a security risk that has been evidenced by numerous security teams [9][10]. Indeed, a study conducted by Computer World revealed that.

nearly 80% of a company's employees' passwords could be cracked in under 30 seconds by means of a network password cracker. In response to the shortcomings of textual passwords, graphical password authentication methods have emerged, designed to overcome their limitations and vulnerabilities [8]. Drawing on research indicating that humans are better at memorizing images rather than verbal representations, these methods offer a more intuitive and user-friendly approach to authentication [3][5]. Image-based passwords have demonstrated an improved ability to be recollected over longer periods of time, even without frequent activation, and can be made complex and secure.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

However, these methods are also subject to Visual Hacking (SSAs), whereby passwords, PINs, and other sensitive personal information are obtained through direct observation or video capturing techniques

II. LITERATURE SURVEY

A. H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme This paper proposes a new method for authentication that combines both text and graphics to provide a more resistant to attacks and user-friendly approach [1] to password authentication. This approach seeks to address the limitations of textual passwords, which can be easily compromised through shoulder-surfing attacks, where an intruder obtains a user's credentials by watching them enter it on their device. The S3PAS scheme creates a grid of images and prompts the user to select certain images in a specific order, while also requiring them to enter an alphanumeric password [1][5]. The position and dimension of images are randomized on each login attempt, and the user is prompted to choose different images and positions each time. This makes it difficult for attackers to replicate the login sequence, even if they are able to observe the user's screen during login. The paper describes the implementation of the S3PAS scheme and evaluates its security and usability [1]. They conclude that the S3PAS scheme is resistant to shoulder-surfing attacks, scalable to large user bases, and provides a user-friendly authentication experience.

B. A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier torecall than words?" Empirical evidence suggests that individuals have a superior free verbal recall of objects or pictures when compared to their corresponding labels or names [2]. The aforementioned phenomenon has garnered the attention of researchers, given that verbal coding processes alone appear to be insufficient in explaining it. If verbal processes were the sole factor at play, one would anticipate words to be
recalled more effectively than images, owing to their quicker readability [2]. However, since pictures are remembered better, it implies that nonverbal processes play a role in the retrieval process. Four theoretical possibilities have been proposed to explain this phenomenon, but none have been widely accepted as the correct explanation. Previous research has shown that nouns are better recalled when presented alongside coloured pictures than when presented alone, but it is not entirely relevant to the present problem of why pictures are better remembered than names.

C. A. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Cybersecurity primarily relies on the use of passwords to verify the authenticity of human users. Unfortunately, users often encounter difficulties in remembering passwords, particularly when choosing secure ones that are long and random. Hence, individuals frequently resort to adopting frail and precarious passwords. However, graphical passwords that involve selecting images in lieu of typing alphanumeric strings, provide a potential remedy to the
issue of formulating passwords that are both impregnable and easy to recall. In this study, they present Pass Points, a novel graphical password framework which is more resilient. We detail the findings of an empirical inquiry that juxtaposes the adoption of Pass Points [3] against the deployment of alphanumeric passwords. During investigation, participants generated and rehearsed either an graphical or alphanumerical password [3], followed by three subsequent longitudinal tests that panned over a six week period to enter their password. The findings demonstrate that those who opted for graphical passwords devised an authentic password with comparatively less difficulty than their alphanumeric counterparts. However,
the graphical password users encountered prolonged durations and a higher frequency of incorrect password entries while familiarizing themselves with their passwords than those who utilized alphanumeric passwords.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

A. Hybrid Colour Shuffling

This solution involves two steps to confirm the user's identification. The technique uses three concentric rings, each divided into eight pieces. The outermost circle contains numbers, the centre circle contains colours, and the interior circle contains eight-character random strings. During the registration procedure, the user assigns a unique number to their selected colour. To authenticate, the user must rotate the circles until the allotted number and the central circle's matching colour match. Following that, they must select a random string composed primarily of the characters they entered in their password during registration. If both pairs are correct, the user's authentication is valid. An additional level of protection is supplied.

B. Hue box Scheme

This strategy improves Hybrid Colour Shuffling. The Hybrid Colour Shuffling Technique is more secure than previous techniques since it requires users to enter a username and password during registration. The password consists of three components: text, rank, and colour. Users must also submit a valid email address in case they forget their password, in addition to their login details. When the user logs in, the system displays a table with numbers, colours, and randomly organized characters. The numbers are fixed, and buttons can be used to move the other two rows. To login, users must first align their preferred colour under their chosen rank and then confirm it using the colour left and right shift buttons. The next phase needs users to use the text left and right shift buttons to align each character of their password with the mandated text and confirm each one individually. When users click the login button at the end, a password is created for the session. If the user forgets his or her password, it will be delivered to their registered email address.

C. Colour-Code Combination System

This paper proposes a hybrid user authentication technique that combines text and colours to improve security, usability, and stability. During registration, the user selects three different colours and rates them individually from 0 to 9. The colour-coded combination is kept in the database as the user's password. During login, the system displays the colours randomly and asks the user to rate them correctly for successful authentication. The system also displays different colour combinations each time the user logs in, improving security against dictionary attacks.

DISADVANTAGES OF THE EXISTING SYSTEM

Complexity and Learning Curve: Both the Hue box Scheme and the Hybrid Color Shuffling involve multi-step verification procedures, which may make it more difficult for users to get started, especially those who are not as tech-savvy. Users may struggle to precisely align text and colors, causing them to become frustrated and abandon the authentication procedure.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

Limited Accessibility: These systems rely heavily on visual elements such as colors and graphical representations, which may cause problems for users with visual impairments or color blindness. Additional features or various authentication procedures may be required to enable accessible for all users, significantly complicating the system.

Error-prone: Because color perception is subjective, the Color-Code Combination System, which needs users to rate colors correctly at login, may cause issues. Even if users are genuine, they may struggle to accurately assess colors on a frequent basis, perhaps leading to authentication failures.

Enhanced susceptibility to Shoulder Surfing: Shoulder surfing attacks, in which unauthorized parties view users' activity and potentially take control of their accounts, may be easier to perform on graphical authentication systems. Users may be vulnerable to such threats if color-coded combinations or graphical representations are shown in public places.

Difficulties with Password Recovery: Although the Hue box Scheme includes an email-based password recovery solution, email password storage and transfer pose security risks. Users may also forget the specific activities required for authentication, making it difficult to recover passwords or access their accounts.

B. PROPOSED SYSTEM

When comparing the three current systems based on authentication levels, accuracy, and usability, the suggested system comes out on top. Three rounds of authentication password verification, colour matching, and pattern matching are incorporated in the suggested system. A user must provide their username and password in the first layer while attempting to log in on their own. If a user is found, they will move on to the colour matching stage of authentication. The user is required to select six colours in the same order as when they registered. If all six colours match, the user will be able to proceed to the next step of the authentication process.

This category offers the highest level of safety. The pattern matching level, in which the user must draw a pattern, is the final stage of authentication. The user must draw the similar pattern that they drew during the registration procedure in order to prove their identity. Every user is unique, and everyone follows a particular pattern. This is how an individual logs into the system.

IV.SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

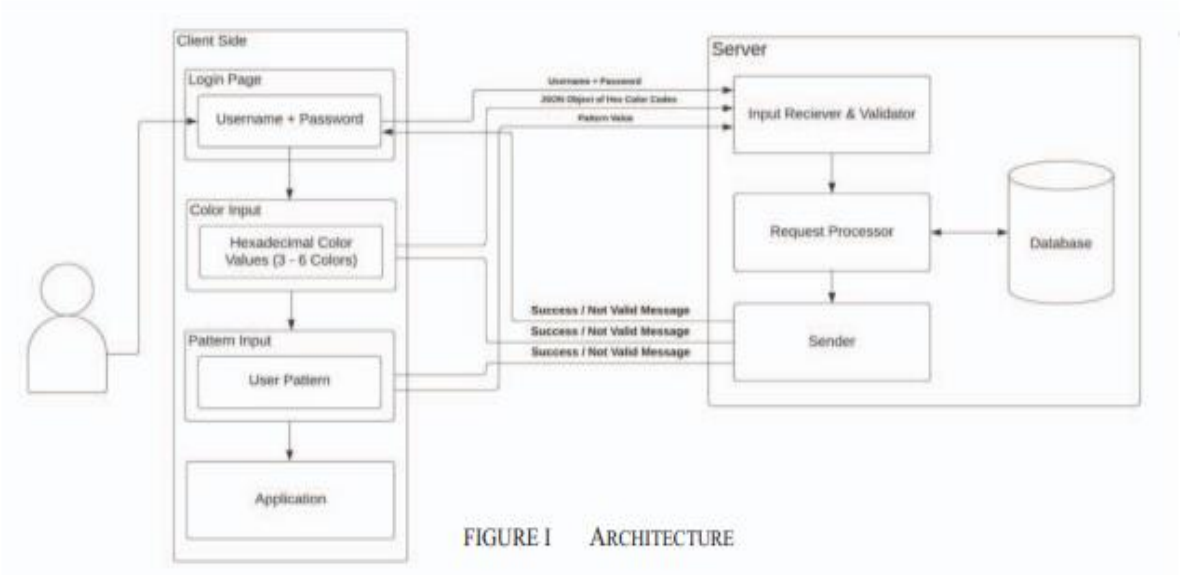

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

System Design and Implementation:
Detail the architecture and components of the graphical password authentication system. Explain the three-layered security mechanism, color, and pattern matching functionalities. Describe the password verification process and the integration of graphical passwords.

User Testing and Evaluation:
Present the methodology for user testing and evaluation. Describe test scenarios, criteria, and data collection. Analyze the results and findings, including user feedback.

Security and Usability Analysis:
Evaluate the system's resistance to Visual Hacking. Compare it with existing authentication systems. Assess user-friendliness and satisfaction through usability testing.

Conclusion and Future Directions:
Summarize key findings and project contributions. Discuss the implications for security and usability. Suggest potential applications and areas for future research.

These modules provide an overview of the project, its implementation, testing, analysis, and the conclusion, and they should help you structure your work effectively.

VI . RESULTS AND DISCUSSION

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

Along with password verification, it includes color and pattern matching features, which provide significant challenges to potential attackers. The prototype's trial results demonstrate that the system can withstand Visual Hacking while maintaining a high level of security and usability.

The accuracy of the system is the measured by calculating how many attempts does a valid user take to successfully authenticate themselves. This parameter reflects how easily the user can authenticate themselves. From Table, we can infer that most of the users who use our system has more authenticated themselves quickly and thus the proposed system has the highest accuracy when compared with other existing systems. The same is represented in the Fig.

S. No	System Name	Percentage of user logged in within 2 attempts
1	Hybrid Color Shuffling	80.00
2	Huebox Scheme	86.67
3	Color-Code Combination	93.33
4	Proposed System	96.67

Table 1. Accuracy

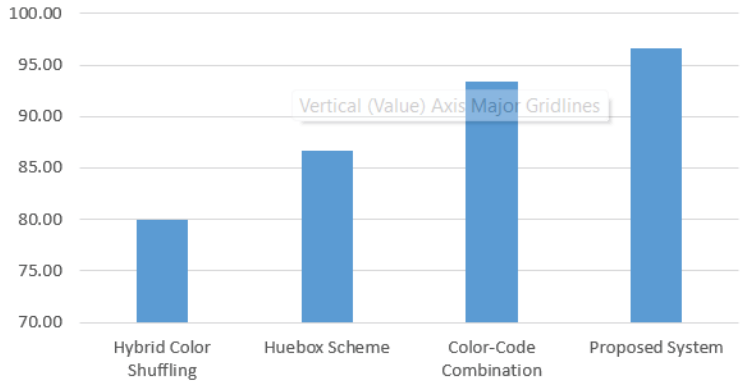

Fig 2. Accuracy comparison graph

S. No	System Name	Authentication levels
1	Hybrid Color Shuffling	2
2	Huebox Scheme	2
3	Color-Code Combination	1
4	Proposed System	3

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

Fig 3. Authentication Levels

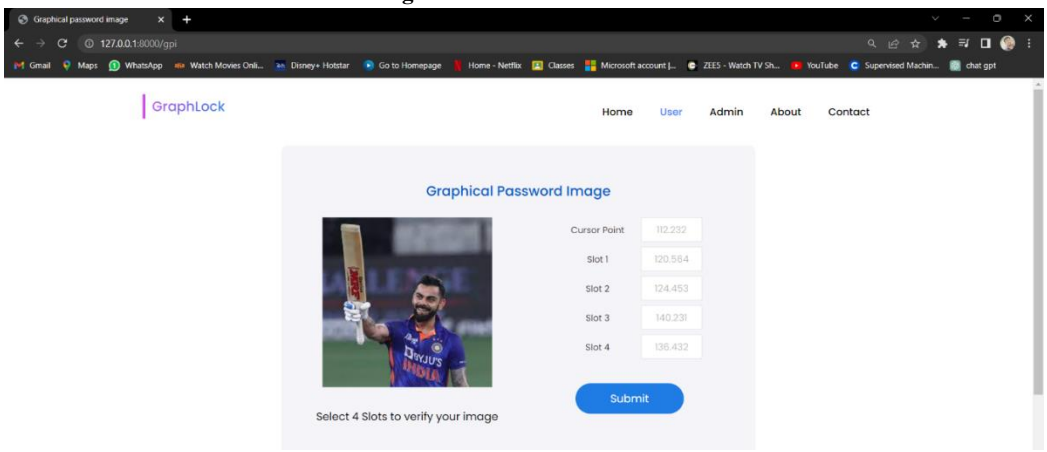

Fig 4. Proposed graphical Authentication

VI I.CONCLUSION AD FUTURE WORK

The suggested Triggered Click Points (TCP) approach shows promise as a user-friendly and memorable graphical authentication technique. TCP outperforms Pass Points in terms of usability by leveraging user recognition and memory triggers for new pictures. Using search pictures and remembering a single click-point per image is easier than remembering an ordered series of clicks. on a single picture. TCP provides a more secure alternative to Pass Point. TCP increases attacker burden by requiring them to obtain picture sets for each user and perform hotspot analysis. In the future, we can include challenge response interactivity. During challenge response exchanges, the server will provide a challenge for the client, and the client must respond in accordance with the conditions provided. If the response is accurate, access will be given. We can limit a user's ability to input incorrect passwords.

REFERENCES :

[1] Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In 21st international conference on advanced information networking and applications workshops (AINAW'07) (Vol. 2, pp. 467-472). IEEE.

[2] Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words?. Psychonomic Science, 11(4), 137-138.

[3] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies, 63(1- 2), 102-127.

[4] Martinez-Diaz, M., Fierrez, J., & Galbally, J. (2015). Graphical password-based user authentication with free-form doodles. IEEE Transactions on HumanMachine Systems, 46(4), 607-614.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

[5] Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2016). A shoulder surfing resistant graphical authentication system. IEEE Transactions on Dependable and Secure Computing, 15(2), 180-193.

[6] Shah, M., Naik, R., Mullakodi, S., & Chaudhari, S. (2018). Comparative analysis of different graphical password techniques for security. Int Res J Eng Technol (IRJET), 5(4), 1873-1877.

[7] Nali, Deholo, and Julie Thorpe. "Analyzing user choice in graphical passwords." School of Computer Science, Carleton University, Tech. Rep. TR-04-01 (2004).

[8] Jermyn, Ian H., Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. "The design and analysis of graphical passwords." USENIX Association, 1999.

[9] Bousfield, Weston Ashmore, J. Esterson, and Gerald A. Whitmarsh. "The effects of concomitant coloured and uncoloured pictorial representations on the learning of stimulus words." Journal of applied psychology 41, no. 3 (1957): 165.

[10]Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. "Authentication using graphical passwords: Effects of tolerance and image choice." In Proceedings of the 2005 symposium on Usable privacy and security, pp. 1-12. 2005.

[11]Tari, Furkan, A. Ant Ozok, and Stephen H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." In Proceedings of the second symposium on Usable privacy and security, pp. 56-66. 2006.

[12]Stobert, Elizabeth, Alain Forget, Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. "Exploring usability effects of increasing security in click-based graphical passwords." In Proceedings of the 26th Annual Computer Security Applications Conference, pp. 79-88. 2010.

[13]Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords." The Rutger Scholar 4 (2002).

[14]Stobert, Elizabeth, and Robert Biddle. "Memory retrieval and graphical passwords." In Proceedings of the ninth symposium on usable privacy and security, pp. 1-14. 2013.

[15]Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." In 21st Annual Computer Security Applications Conference (ACSAC'05), pp. 10-pp. IEEE, 2005.