

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

A SECURE HYBRID AUTHENTICATION SYSTEM

Mecwan Ujjawal Rajkumar¹, Mr. Lokendra Singh Songare²

¹Student, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India

²Assistant Professor, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India

ABSTRACT

Numerous shoulder surfing techniques have been developed, however predictable secret word patterns are now vulnerable to dictionary assaults, eve dropping, and shoulder surfing. At the same time, text passwords are the most often utilised authentication publicising strategy. In previous years, there were some graphical password schemes that were intended. The majority of We have suggested word-based graphical password schemes since users prefer word-based passwords over pure graphical ones. Unfortunately, no hybrid digital graphical password system is created by any of the current approaches. In this study, we propose an enhanced graphical password that is primarily text-based, numerical-based, shoulder surfing resistant, and also employs additional techniques such as social engineering resistance, eves dropping, and dictionary attack resistance through the use of colours. The operator can observe the proposed system's security, usability, and resilience to different threats by logging in to the system in a reliable, easy, and efficient manner.

KEYWORDS: Authentication, hybrid password.

INTRODUCTION

Text-based passwords are the most often used authentication method. As a result, it is vulnerable to well-known attacks such as shoulder surfing, dictionary attacks, social media attacks, and eve dropping. Long and unexpected passwords might make the system secure. However, this might lead to issues, such as the inability to remember those words. End users tend to use short passwords or ones that are easy to remember, according to surveys. These words are fatefully easily split up. Today, a variety of techniques are available, such as biometrics and graphical passwords, each with certain drawbacks. Although they have been proposed, biometric password approaches like fingerprints and face recognition are not yet widely used. The main drawback of this approach is that such The entire recognition procedure can be time-consuming, and accommodations might be costly. the quantity of predicted graphical password techniques from the previous era. However, the majority of techniques are vulnerable to shoulder surfing attacks, which are starting to pose a significant problem. It has been projected that some graphical password patterns are resistant to shoulder-surfing, but they also have certain drawbacks, such as usability issues or lengthy login times. By keeping an eye on the user over his shoulder as he enters his password, the adversary can employ the shoulder surfing attack to obtain the user's password. Beginning that same year, a variety of hybrid graphical password techniques included. There are advantages and disadvantages to each of the several grades of resistance to shoulder surfing that have been predicted, such as [2] [3] [4] [5] [6] [7] [8] [9]. In response to shoulder surfing, Sobrado and Birget [1] suggested three graphical password techniques that are resistant to shoulder surfing. Considering that the majority of users prefer text passwords over graphical ones, Zhao et al. [10] suggested S3APS, a text-based graphical password technique that prevents shoulder surfing. To get the session password in S3PAS, the user must provide his text password on the login screen. Additionally, Zhao et al.'s approaches' login process is challenging and uninteresting. Following that, other graphical password techniques that are resistant to textual shoulder surfing have been proposed, including [11] [12] [13] [14] [15]. Unfortunately, none of the current graphical password methods that prevent textual shoulder surfing are secure and efficient. In this report, we will propose a better textual based shoulder surfing resistant graphical password structure by with colors. The operation of the proposed methods is easy and simple to read for users aware with word-based words. The user can effortlessly and professionally to log in, the system without using any physical keyboard.

RELATED STUDY

Three shoulder surfing-resistant graphical password schemes—the Movable Frame, Intersection, and Triangle methods—were put out by Sobrado and Birget [1] in 2002. The Movable Frame and Intersection approaches, however, also have a significant failure rate. The user must choose and commit to memory a number of passes-icons as his words while using the triangle approaches. The user must successfully complete the predefined amount of tasks at the time of signing in. Each challenge requires the user to choose three passes-icons from a group of randomly chosen icons that are shown on the login screen, then snap inside the invisible triangle those three passes-icons form. To verify the user's legitimacy, Profound Dhamija [2] provided a graphical verification

mechanism in which the user must recognise pre-defined pictures. During registration, the user selects several photographs from a large collection of random pictures in this system. The user must identify the previously shot photos for group verification at the time of logging. multiple photos, as seen in figure 1. Shoulder-surfing can occur with this technique. [3] Wiedenbeck et al. The Convex Hull Click technique (CHC), which was proposed in 2006, is an improved version of the Triangle technique that offers more serviceability and protection. The user must correctly respond to a few challenges throughout the login process. The user must locate one of the three pass-icons on the login screen for each challenge, then click inside the invisible convex hull created using all of the displayed pass-icons. However, the Convex-Hull Click scheme's drawback is its potentially excessively lengthy login time. A shoulder surfing-resistant graphical password system with colour login was presented by Gao et al. [4] in 2009. The backdrop colour is a functional problem for reducing the login time. However, the password space is very limited and the likelihood of an accidental Colour Login login is too great. Additionally, Yamamoto et al. [9] suggested a shoulder TI-IBA is a graphical password system that is resistant to browsing and has icons that are displayed both temporally and spatially. The user can locate his pass-icons more easily and TI-IBA is less embarrassed by the screen size. Fortunately, TI-IBA does not have a strong defence against unwanted logins. Additionally, some users could find it difficult to locate their pass-icons temporarily on the login screen. The majority of consumers are aware that traditional text-based password verification techniques are shoulder surfing-resistant. S3PAS is a text-based shoulder surfing resistant graphical password system that Zhao et al. [10] presented in 2007. The user must first choose his text password and then adhere to a set of rules to To hold a session password to access the system, blend his textual password. At the same time, Zhao et al.'s login procedures are convoluted and dull. In 2011, Sreelatha et al. [12] also suggested a graphical password system that uses colours and is text-based and resistant to shoulder surfing.

PROBLEM STATEMENT AND PROPOSED SOLUTION

To discover a solution for security from shoulder-surfing without encountering any further challenges. To overcome the shoulder-surfing assault, use a variety of authentication procedures without adding unnecessary complexity. The proposed scheme is divides into 3 phases: The registration stage, the login stage and the verification stage, which can be designated as in the following.

Stage 1:- Registration

At the time of registration, the user enters his username. The maximum length of the username is 8, and it can be referred to as a secret pass. The secret pass has an even number of characters. A session password is generated, and the user is then prompted to set his password.

Stage 2:- Login Stage

When the user enters his password during the login process, an interface with a virtual keyboard appears. The virtual keyboard has alphabets, numbers, and symbols. They are arranged freely on the virtual keyboard, and the interface varies with each login. The user inputs the password. The user must consider his secret pass in terms of pairs. The session password comprises of characters and digits.

Stage 3:- Verification Stage

If the account is not successfully verified three times in a row during this Phase, it will be inactivated, and the system will send an e-mail to the user's registered e-mail address with the secret link that the valid user can use to reactivate his inactivated account.

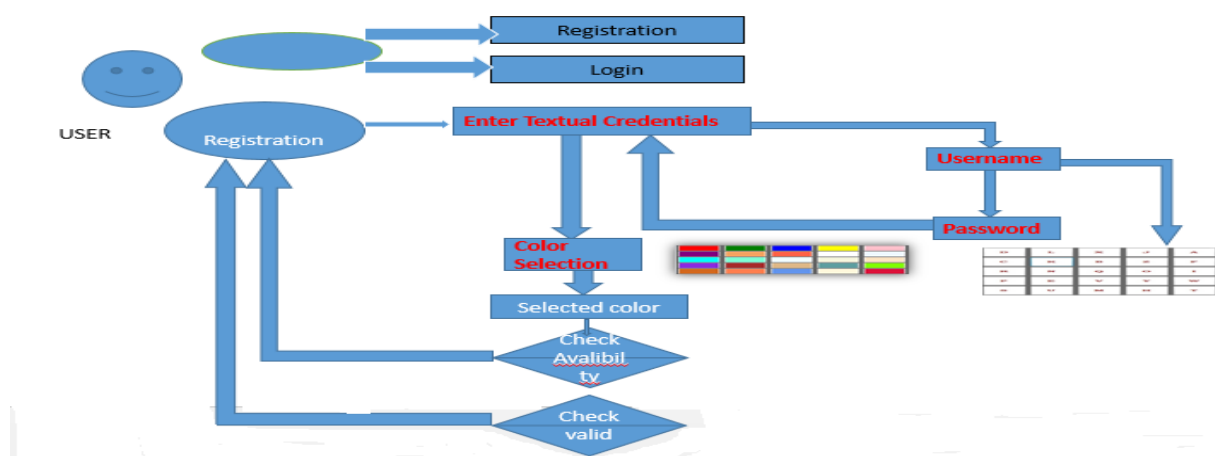


Figure 1: System Architecture

RESULTS ANALYSIS

In this section, performance of proposed scheme evaluated. Additionally, a performance comparison has also been presented.

Authentication schemes	Textual Passwords	Image based Passwords	Token based passwords	Bio metric passwords	Proposed Schemes
Usability	very high	High	Less	very less	very high
Resistance to accidental login	Possible	Possible	Possible	Possible	Quite Possible
Attacks	Brute force, dictionary , Guessing	shoulder surfing, guessing	Forgery	Forgery	no matter
Password space	quite less	Less	no matter	no matter	quite less
Resistance to Shoulder surfing	No	Less	Less	Less	High
Time to login	Low	Moderate	Moderate	High	Moderate
Flexibility	Moderate	High	Low	very low	Easy
Recovery	Easy	Easy	Hard	Difficult	Easy

CONCLUSION

In this paper, we developed a simple text-based graphical password that is immune to shoulder surfing assaults, allowing the user to finish the login procedure with ease and efficiency. The proposed technique is straightforward and easy to learn for users who are familiar with textual passwords. The user may simply and swiftly log into the system using the on-screen keyboard. Finally, we investigated the resistance of the proposed approach against shoulder surfing and accidental login.

REFERENCES

- [1] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
- [2] R. Dhamija, and A. Perrig, "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
- [3] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.
- [4] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.
- [5] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
- [6] B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumeric password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.
- [7] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105111 .
- [8] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: shoulder surfing safe login," Proc. of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.
- [9] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.
- [10] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shouldersurfing-resistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188194.
- [11] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proc. Of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.
- [12] B. R. Cheng, W. C. Ku, and W. P. Chen, "An efficient login-recording attack resistant graphical password scheme— SectorLogin," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.



- [13] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011.
- [14] S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. "A new shoulder-surfing resistant password for mobile environments," Proc. Of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.
- [15] Z. Imran and R. Nizami, "Advance secure login," International Journal of Scientific and Research Publications, vol. 1, Dec. 2011.