

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

AUTHENTICATION SECURELY THROUGH A 3D IMAGE PASSWORD

Mecwan Umang Rajkumar¹, Mr. Arpit Solanki²

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

Currently, computers and the internet have become a crucial aspect of everyone's lives. Various applications can send and store vast amounts of critical data. User-friendly programs are given for easy use. Various approaches are developed to secure such apps. Authentication methods include textual passwords, graphical passwords, and colour passwords. But these authentication techniques are vulnerable to a variety of assaults. Many times, the username is simple, allowing the attacker to quickly remember it and guess the password. So in the suggested system, we created three authentication systems that offer a secret username, a graphical password, and a colour password. After verifying the graphical password, the user can enter the secret username and the colour password. After successfully verifying three schemes, the user is able to access the application. So the new approach will give strong security by combining graphical passwords with secret usernames and colour passwords.

KEYWORDS: Authentication, graphical password, colour password, security, secret username, PCCP.

INTRODUCTION

In today's environment, all applications use an authentication mechanism for security reasons. However, they are still employing the traditional approach of textual passwords. However, in most cases, the password can be hacked and critical information taken. To give high security to apps, new techniques need be developed. The graphical password is the best option for this. The hackers are unable to predict where the photos will be clicked.

The programs are only secured with passwords, although they can be secure with both a secret username and a password. According to the study, people can retain graphical information for longer periods of time than alphabetic information [9]. According to psychological studies, the human mind remembers visuals more easily than letters or digits. Critical textual passwords must occasionally be written or stored, but graphical passwords do not. Most low-literacy users also utilise various programs, and textual interfaces are inaccessible to them.

Many individuals can choose intricate textual passwords that are difficult to remember. Every time a user recalls their password, they must priorities security over their necessity in order to complete their work. The secret user name and graphical password are good options for alphanumeric passwords since they provide great protection. The graphical password method is suitable for all types of users, including those with limited computer experience. The user does not have to remember the precise coordinates every time. For this, a tolerance region should be built around the pixel, allowing the user to select pixels near the recorded pixels. To choose small locations on the image, use the image viewport. To save storage space, choose smaller image sizes.

Currently, the default authentication mechanism is alphanumeric passwords. Alphanumeric passwords are not particularly safe or easy to remember. Another key point to note is that individuals have repeatedly recalled their password. To complete their work, users must priorities security above and beyond their immediate needs. Implementing secure and efficient authentication schemes is not simple. The transition to graphical passwords necessitates the establishment of secure graphical password definitions in order to improve user convenience while also limiting the number of successful attacks on such schemes. The purpose of a new authentication system is to let users choose a secret username and a strong password. Graphical passwords are an alternative to alphabetic passwords. Graphical passwords employ graphics or representations of images as passwords. Pictures are easier for human brains to recognize than words. User Should effortlessly and swiftly complete the login process without fear of shoulder surfing assaults.

RELATED STUDY

The most prevalent type of authentication is textual authentication. Several graphical approaches are also utilised for authentication. Some of the existing systems are listed below.

Resistance to shoulder surfing attacks is a significant concern. [2] It proposed a superior text-based, shoulder surfing-resistant graphical password system using colours. The method was created to avoid accidental logins in

the system. The compelling feature [3] is added to the cued click location to generate a random password. The strength [4] of graphical authentication systems is evaluated based on their performance. They genuinely compare the traditional text-based password system to graphical password systems. They also present results showing that graphical systems are more secure than traditional ones. Two authentication systems based on text and colours [5] are used to generate graphical passwords. These methods are resistant to shoulder surfing. They also suggested that the new scheme will be immune to shoulder surfing attacks. Two algorithmic approaches [6] based on security requirements are outlined. The ways used to generate the session password are text and colour. Text passwords pose significant security risks [7]. Session passwords are generated using the paired-based and hybrid textual authentication techniques. It resolves all security difficulties with text passwords. The PCCP approach is utilised for graphical passwords. The new approach known as secret drawing is used in conjunction with PCCP [11] to ensure security.

PROBLEM STATEMENT AND PROPOSED SOLUTION

Once a password has been chosen and learnt, the user must be able to remember it in order to log in. However, people routinely forget their passwords. People forget their passwords for various reasons, including decay and interference. Items in memory may compete with a password, preventing an accurate recall. Passwords that are not used frequently are more likely to be forgotten. A major difficulty is that people have many passwords for computers, networks, and websites. The huge number of passwords increases interference and is more likely to result in password forgetting or confusion. This suggested solution is based on three authentication schemes, which operate together to give increased security to the system or application. During the verification step, the PCCP, Grid-Based, and Colour-Based authentication schemes provide three layers of security. The first layer has PCCP; the second layer contains Grid Based Authentication; and the third layer contains Colour Based Authentication.

If a user is successfully verified by the first layer, i.e. PCCP, it gains access to the second layer. If a person is successfully verified in the second layer, which is Grid Based Authentication, he or she gains access to the third layer. In the third layer, Colour Based Authentication, if the user is successfully verified, he or she is then granted access to the application or system. The proposed system provides 3D (three-dimensional) security to the application. This system is designed to provide robust security by utilising a grid-based authentication technique for usernames, graphic passwords, and color-based authentication.

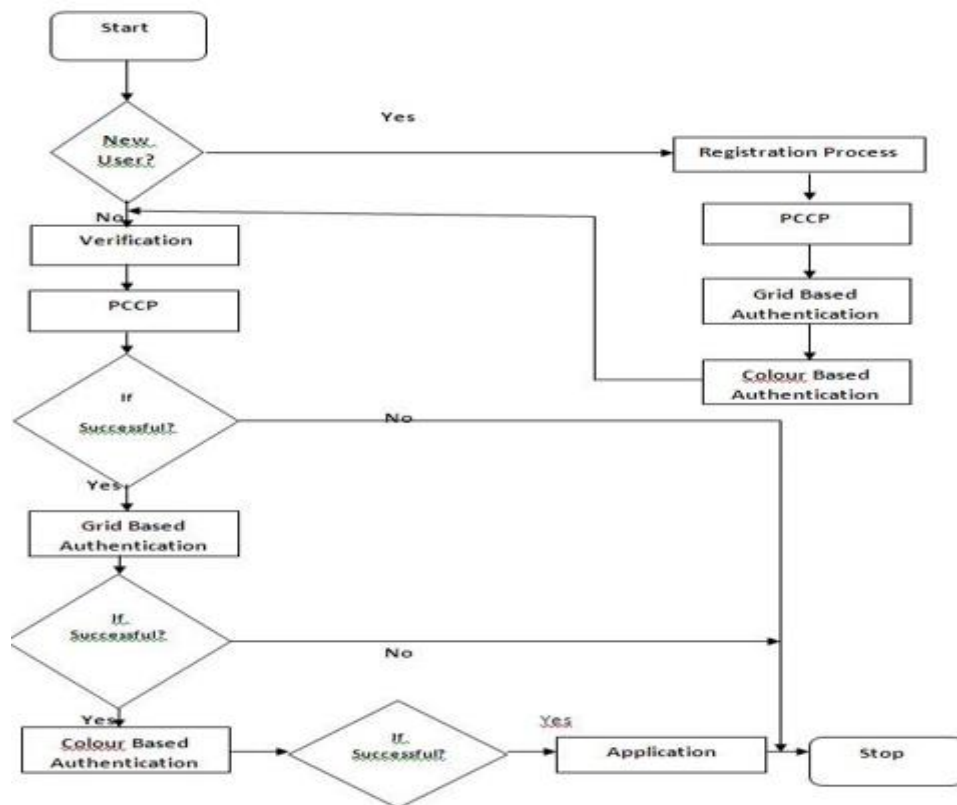


Figure 1: System Architecture

RESULTS ANALYSIS

Figure: 2 shows the time required for username and Figure: 3 shows the strength of graphical password.

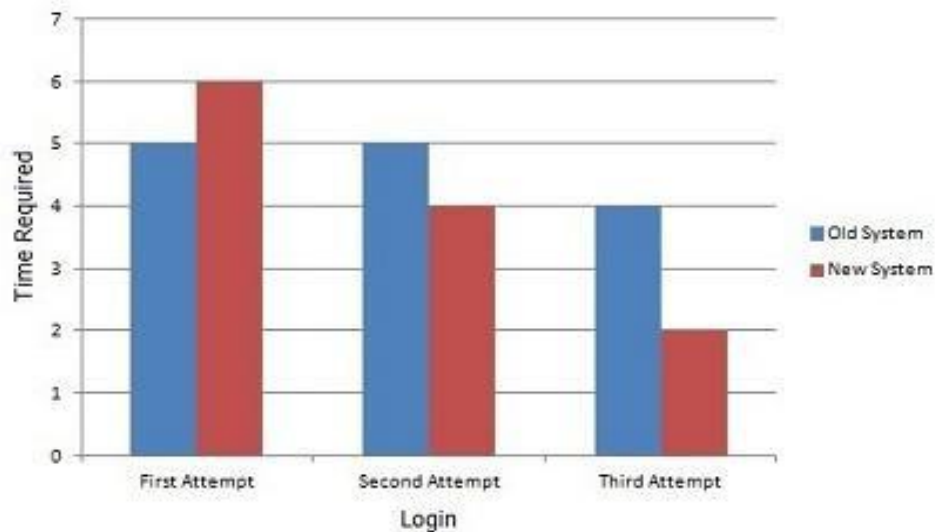


Figure 2: Graph showing time required for username

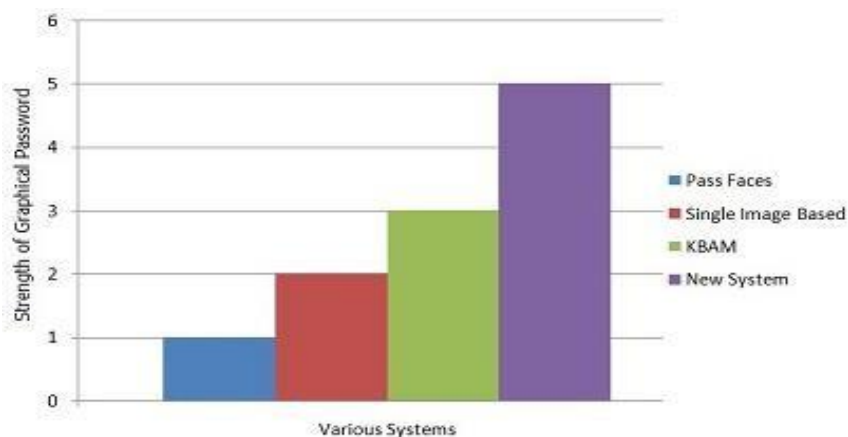


Figure 3: Graph showing strength of graphical password

CONCLUSION

The system provides great security through the use of a secret username, graphic password, and colour password. The secret username can be provided by a grid-based system, graphical password authentication can be provided by using PCCP, and colour passwords can be provided by a color-based intent city matrix. These systems are resistant to dictionary and brute force attacks, as well as shoulder-surfing. The suggested approach addresses the numerous issues with the existing authentication mechanism. It can also help users with security by providing a secret username, graphical password, and colour password. This system will function as an algorithm for future authentication schemes.

REFERENCES

- [1] Nesrine Kaaniche, Maryline Laurent "A Secure Client Side Deduplication Scheme in Cloud Storage Environments" 6th International Conference on New Technologies, Mobility and Security Year 2014
- [2] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme" 2nd International Symposium on Next-Generation Electronics (ISNE) IEEE 2013
- [3] Uma D. Yadav, Prakash S. Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM" International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013) IEEE 2013

- [4] Karen Renaud, Peter Mayer, Melanie Volkamer, Joseph Maguire “Are Graphical Authentication Mechanisms As Strong As Passwords?” Pro- ceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 837–844, IEEE 2013
- [5] Mr. Sagar A. Dhanake, Mr. Umesh M. Korade, Mr.Chetan P. Shi- tole, Mr. Sagar B. Kedar, Prof. V. M. Lomte “ Authentication Scheme for Session Password using matrix Colour and Text” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278- 8727Volume 16, Issue 1, Ver. II, PP 36-42, Jan. 2014
- [6] Rohit Jagtap, Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher “Authen- tication schemes for session password using color and special characters” International Journal of Innovations Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 3, Issue 2 April 2014.
- [7] M Sreelatha, M Shashi, M Anirudh, M D Sultan Ahamer, V Manoj Kumar “Authentication Schemes for Session Passwords using Color and Images” International Journal of Network Security Its Applications (IJNSA), Vol.3, No.3, May 2011.
- [8] Yuxin Meng “Designing Click-Draw Based Graphical Password Scheme for Better Authentication” Seventh International Conference on Net- working, Architecture, and Storage, IEEE 2012.
- [9] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare “Graphical Password Authentication Cloud securing scheme” International Conference on Electronic Systems, Signal Processing and Computing Technologies, IEEE 2014.
- [10] Tara H R, Usha T, Ganeshayya I Shidaganti “Knowledge Based Authen- tication Mechanism Using Persuasive Cued Click Points” International Journal of Engineering Research Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 6, June – 2013.
- [11] P. R. Devale, Shrikala M. Deshmukh, Anil B. Pawar “ Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme” In- ternational Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.
- [12] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P. C. Van Oorschot “Persuasive Cued Click-Points: Design, implementation, and evaluation of a Knowledge based authentication mechanism” IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE 2011.
- [13] Mokgadi Rasekgala, Sigrid Ewert, Ian Sanders, Thomas Fogwill “Re- quirements for Secure Graphical Password Schemes” IST-Africa Con- ference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, ISBN: 978- 1-905824-44-1-2014.