iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61183

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

A Recognition-Based Graphical Password System for Enhanced User Authentication

Mrs.Ch.Naga Lakshmi Geetha[1] , A Sowmya Sri Satya Devi[2], J Harshita Maha Lakshmi[3], Suvvari Aravind[4], A Sri Ramanna Dora[5]
[1]*Assistant Professor* , [2, 3, 4, 5]*B.tech Students Department of Information Technology, Pragati Engineering College, Surampalem , Andhra Pradesh, India*

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: Authentication, Graphical Passwords, Visual Hacking, Shoulder Surfing

I. INTRODUCTION

Textual passwords, which blend capital and lowercase letters with digits to increase resistance against brute force attacks, have been the traditional authentication method for decades. Despite their widespread use, these passwords are exceedingly difficult to remember and retain because of the level of complexity required to make them really secure. Instead of utilizing a random alphanumeric sequence, users usually succumb to the temptation of using passwords that are either too short or easily guessed from the dictionary.

People using the same login credentials for several accounts is a worrying trend, exacerbated by the fact that various security teams have demonstrated that this constitutes a security risk. In fact, a Computer World survey discovered that a network password cracker could break around 80% of employee credentials in less than 30 seconds. Graphical password authentication systems were developed in reaction to the limitations of textual passwords, with the goal of resolving their restrictions and shortcomings. Based on research indicating that individuals remember visual information better than verbal descriptions, these strategies give a more natural and approachable method of authentication. Image-based passwords can be made more complex and secure, and they have been demonstrated to be better remembered over longer periods of time—even without frequent activation. Nonetheless, these approaches are vulnerable to Visual Hacking, which collects passwords and other confidential

II. LITERATURE SURVEY

"A scalable textual-graphical password authentication scheme that is resistant to shoulder-surfing" It is widely acknowledged that text passwords are insecure. Because users commonly utilize short or easy-to-remember passwords, attackers can readily crack them. Furthermore, malware, concealed cameras, and shoulder surfing can all attack text-based passwords. It has been suggested that graphic password schemes be utilized rather than text-based ones. Nonetheless, most of them are prone to shoulder-surfing. This paper introduces a Scalable Textual-Graphical Password Authentication Scheme (S3PAS) that is resistant to shoulder surfing. S3PAS seamlessly integrates both graphical and textual password schemes while also providing almost total resistance to spyware, hidden camera, and shoulder-surfing attacks. It can replace existing user password profiles without changing them. Furthermore, it resists brute-force assaults using volatile and dynamic session passwords.

S3PAS shows considerable promise for bridging the gap between graphical and standard text passwords. A brief discussion and proposal for further S3PAS scheme improvements are provided. Additionally, a theoretical analysis of the security level with S3PAS is conducted.

"Why are images more memorable than words?" The first two of the four free recall trials showed that photos of things outperformed names. There were significant differences based on the input serial order, but there was no difference in recall between the two modes in terms of intertriai organization. Trial 1 demonstrated picture superiority for terminal input items, while Trial 2 shown picture superiority for both terminal and early items. The results are explained in terms of concrete (verbal and nonverbal) memory coding.

"User authentication using free-form doodles through graphic passwords" Many portable electronics now rely on basic actions to identify users. This study investigates free-form sketch authentication. Based on dynamic signature verification methodologies, verification systems with dynamic temporal warping and Gaussian mixture models are proposed. The most discriminating traits were studied using a sequential forward floating selection strategy. The impacts of training set size and capture session intervals are also investigated. The DooDB database, which contains passwords from 100 users entered on a smartphone touchscreen, is used for development and validation trials. Random and professional forgeries have comparable mistake rates, ranging from 3% to 8% and 21% to 22%, respectively**.**

"The effects of concomitant colored and uncolored pictorial representations on the learning of stimulus words." Twenty-five stimulus words were provided in three learning situations (a) words alone, (b) words with uncolored pictures, and (c) words with colored pictures) to investigate the impact of varying degrees of compounding signs of the items represented by the words. The hypothesis that "the number of words recalled by Ss should vary positively within limits with the number of simultaneously presented additional signs" was proven to be correct when the number of presentations was held constant.

III. SYSTEM ANALYSIS

A. Existing System

1) Hybrid Color 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 center circle contains colors, and the interior circle contains eight-character random strings. During the registration procedure, the user assigns a unique number to their selected color. To authenticate, the user must rotate the circles until the allotted number and the central circle's matching color 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.

2) Huebox Scheme

This strategy improves Hybrid Color Shuffling. The Hybrid Color 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 color. 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, colors, 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 color under their chosen rank and then confirm it using the color 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.

3) Color-Code Combination System

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

DISADVANTAGES OF THE EXISTING SYSTEM

a) *Complexity and Learning Curve:* Both the Huebox 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.
b) *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.
c) *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.
d) *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.
e) *Difficulties with Password Recovery:* Although the Huebox 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, color 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 color matching stage of authentication. The user is required to select six colors in the same order as when they registered. If all six colors 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.

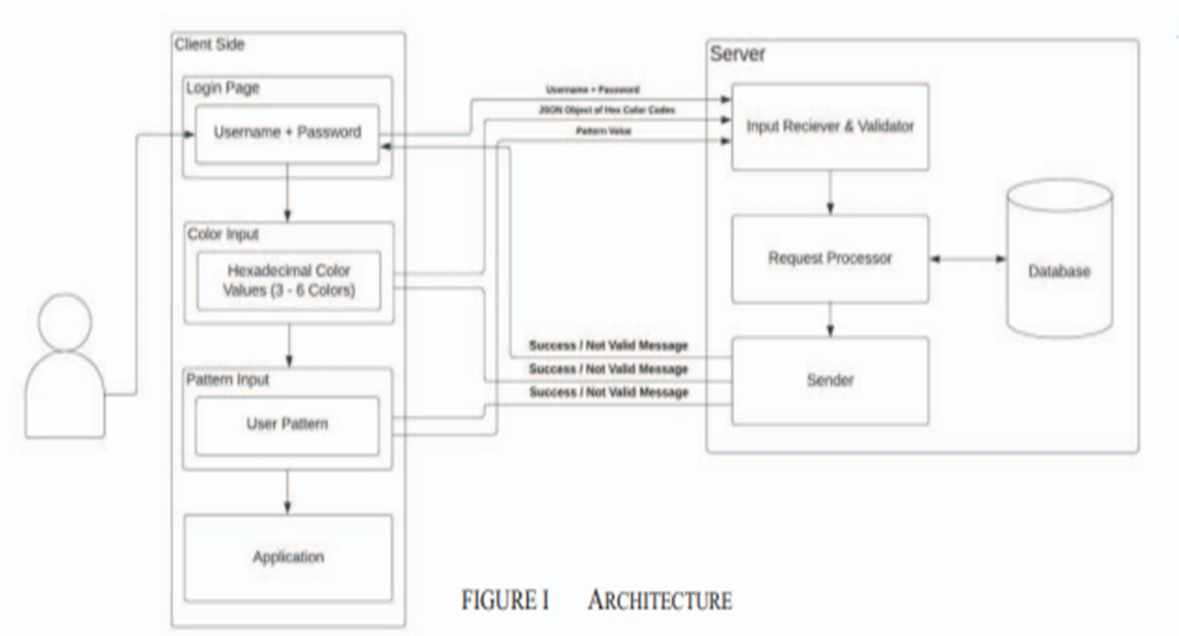


Fig 1. Methodology followed for proposed model

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

V. SYSTEM IMPLEMENTATION

MODULES

Describe the graphical password authentication system's architecture and components.
Explain the purpose of color and pattern matching, as well as the three-layered security method.
Describe the integration of graphical passwords and the password verification process.
Describe your user testing and assessment approach.
Explain the criteria, test scenarios, and data collection.
Examine the results and conclusions while taking into consideration customer feedback.
Analyze security and usability: Determine the system's resistance to visual hacking.
Compare it to the current authentication techniques.
Use usability testing to determine user satisfaction and friendliness.
Highlight significant findings and project contributions.
Discuss how security and usability are affected.
Make recommendations for potential applications and directions for future research.
These modules should help you organize your work more efficiently because they provide an overview of the project, including its implementation, testing, analysis, and conclusion.

VI. RESULTS AND DISCUSSION

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.

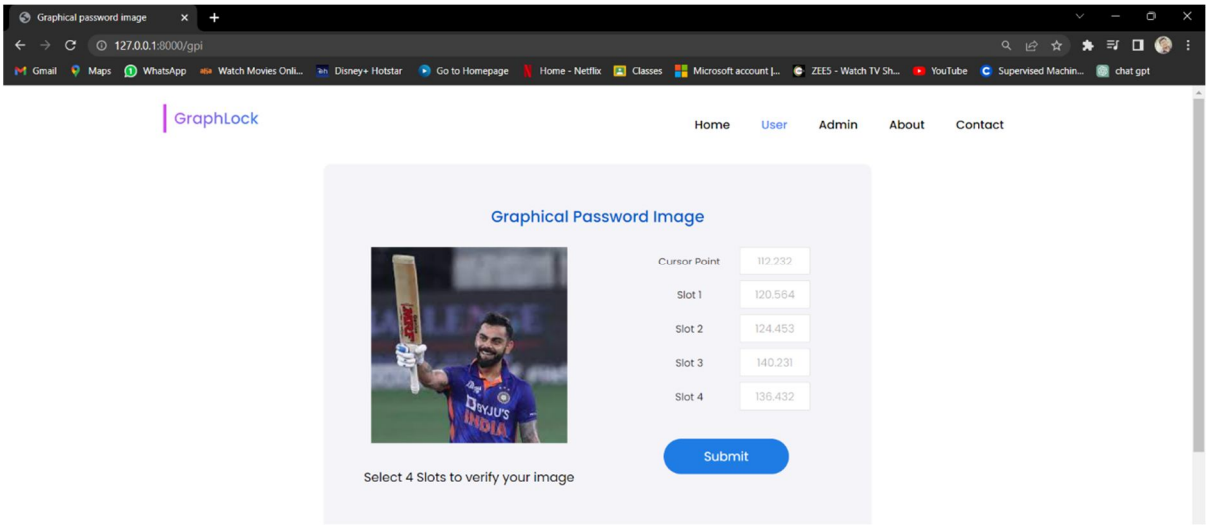


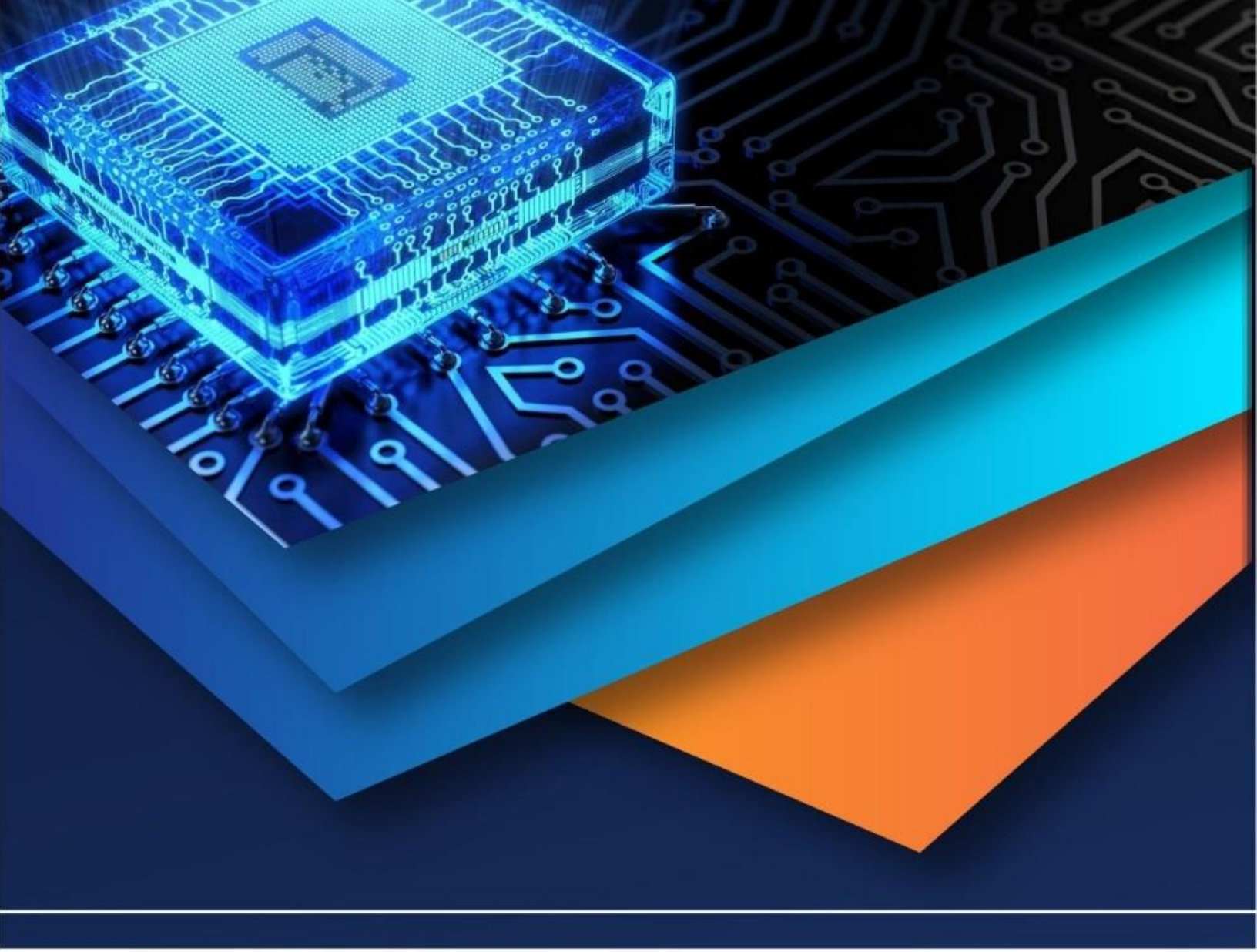
Fig 2. Image Pin-point based Graphical Password authentication system

VII. CONCLUSION AD FUTURE WORK

In particular, by leveraging web services for easy integration with a variety of apps, the proposed authentication system aims to excel at withstanding visual attacks while ensuring user authentication. Thirty unskilled users participated in testing to determine its usefulness, with three primary criteria being usability, accuracy, and the number of authentication layers.
Users spend less time enrolling and logging in than they do with rival systems, showing that the system is more usable. This was evaluated by determining how long it took users on average to accomplish these tasks, and the proposed method worked admirably.
Another essential component, accuracy, was evaluated by calculating the number of attempts required for valid users to successfully authenticate themselves. The majority of users confirmed using the suggested technique quickly, according to the data, indicating its excellent accuracy when compared to other systems.
In addition, the security level of the authentication system was assessed based on the number of authentication layers contained. The recommended system's robustness was proved by comparing it to existing systems, suggesting that its multiple layers of authentication may provide greater security.

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.
[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 colored and uncolored 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY