Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

GRAPHICAL PASSWORD AUTHENTICATION

[1]Ms. Richa Upadhyay, [2]Sneha, [3]Hritika Binawara, [4]Kartik Ashiya

[1]Assistant Professor, Department of Information Technology, JECRC College
[2]B. Tech Student, Department of Information Technology, JECRC College
[3]B. Tech Student, Department of Information Technology, JECRC College
[4]B. Tech Student, Department of Information Technology, JECRC College

ABSTRACT

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics and graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique. The advantages of graphical passwords include heightened security, improved usability, and diversified authentication methods, fostering user-friendly experiences. However, challenges such as susceptibility to shoulder surfing and the lack of standardization pose obstacles to widespread adoption. This approach enhances security by tapping into users' cognitive abilities, rendering the system resistant to common attacks such as brute force attempts and phishing.

Keywords:

[1] INTRODUCTION

Graphical Password Authentication Systems represent a dynamic frontier in cybersecurity, offering a departure from traditional alphanumeric methods by harnessing the innate capabilities of human visual memory. Text password was always tested the memory of the user, so it wasn't good system. Then the invention of biometric authentication system, QR codes and 2 step mobile verification were invented to overtake the disadvantages of the text-based password.

In a graphical password authentication system, the user has to select from images, in a

specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters.

Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords. The allure of graphical passwords lies in their fortified resilience against brute-force assaults, heightened user memorability, and the adaptability to accommodate diverse authentication preferences. Nevertheless, the vulnerability to shoulder surfing and the paucity of standardized practices presents formidable challenges to universal adoption.

[2] RELATED WORK

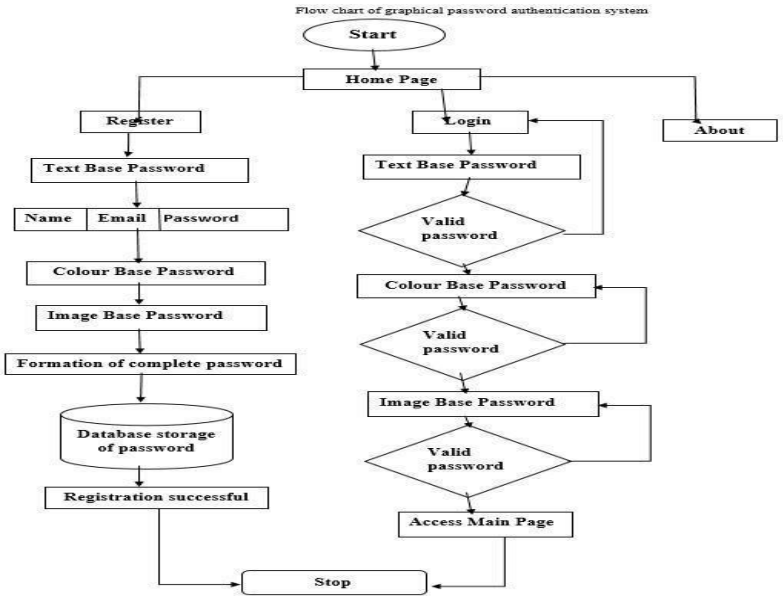
Graphical passwords refer to using images and different color as passwords. The graphical passwords are easier to remember because people remember pictures better than words. The graphical password is more resistant to brute- force attacks. Graphical passwords are more attractive and visual representations that are used in place of text or alphanumeric characters.

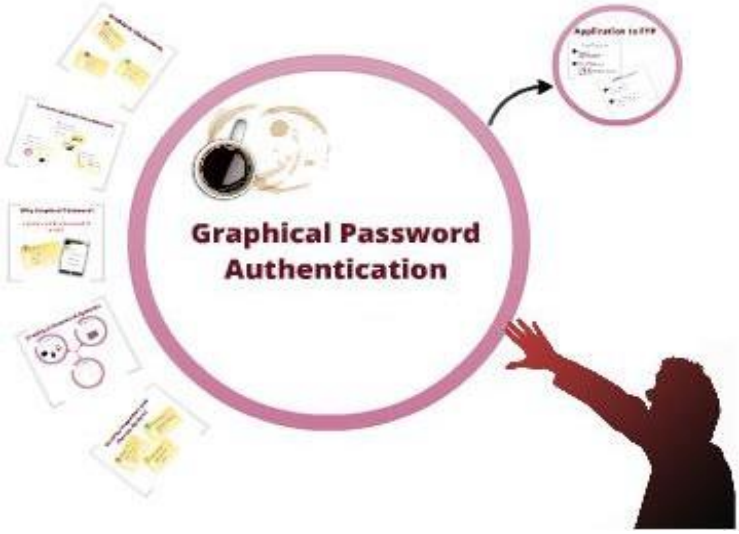
In graphical password we used 2 types of authentications first is color-based and second is image-based authentication, which is easy to recall and difficult to guess and it is the best alternative to the text password. Humans are visual creatures that process and remember visual cues better than most other forms of data, and graphical passwords exploit just that.

Graphical password, user can easily remember so, no need to write down any password to anywhere. And it is very difficult to guess graphical password. Face-recognize is also another type of authentication process which is unique for authentication systems. An early recall-based graphical password method was introduced by Greg Blonder in 1996. In this method, a user generates a password by clicking on different locations on a picture.

Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

In today's information society, the importance of information protection is increasing day by day. One of the things you need to protect your information is the security of information devices. The most used scheme for the security of information devices is the password. The graphical password is more resistant to brute- force attacks.





[3] PROPOSED WORK

1. **Data Collection and Preparation:**

- Dynamic Graph Investigation: Investigate the feasibility and effectiveness of dynamic graphical passwords that change over time or adapt based on user behavior. Dynamic systems can threat certain types of attacks and provide an additional level of security.
- The database stores user profiles securely, including the graphical password data. It must be designed to handle the storage and retrieval of this sensitive information while maintaining robust security measures to protect against unauthorized access.

2. **Model Selection:**

- **User Registration:** The registration process involves users creating their graphical passwords. During this phase, the system guides users through selecting or interacting with graphical elements to establish a unique and secure authentication method.
- **Cross-Platform Compatibility:** Work towards ensuring seamless integration and compatibility of graphical password systems across various platforms, devices, and applications. This involves addressing challenges related to screen sizes, resolutions, and interaction methods.
- **Anti-Shoulder Surfing Techniques:** Research and implement innovative techniques to mitigate the risk of shoulder surfing in graphical password authentication. This could involve incorporating visual obfuscation methods or dynamic elements that make it difficult for observers to discern the user's password.
- **Integration with Biometrics:** Investigate the integration of biometric authentication elements, such as fingerprint recognition or facial recognition, into graphical password systems. This fusion can provide a multi-modal approach, enhancing both security and user experience.

[4] CONCLUSION AND FUTURE WORK

In conclusion, the development and implementation of graphical password authentication systems represents a pioneering approach towards addressing the limitations and vulnerabilities associated with traditional text-based password systems. The presented model and architecture underscore the intricate interplay of components and processes aimed at creating a secure, user-friendly, and adaptable authentication mechanism. In the ever-evolving landscape of cybersecurity, the continued exploration and enhancement of graphical password authentication systems hold significant promise.

The future scope of graphical password authentication systems is marked by exciting possibilities that can revolutionize digital security. One avenue for advancement lies in the seamless integration of various biometric modalities, such as facial recognition and fingerprint scanning, offering a multi-modal approach for heightened user verification. Augmented Reality (AR) and Virtual Reality (VR) technologies hold the potential to transform user interactions, providing immersive and secure authentication experiences distribution of extraterrestrial resources, underscore the need for responsible and sustainable approaches to our cosmic endeavors

Moreover, space exploration and colonization hold profound social and cultural significance, offering opportunities to foster international cooperation and understanding and to inspire future generations to reach for the stars. By examining these dimensions, we can gain a deeper understanding of how space colonization may shape human society and culture in the future. Additionally, further study of the ethical, legal, and policy considerations surrounding space exploration and colonization is needed to develop robust frameworks for governing our activities in space. This includes addressing issues such as space debris mitigation, planetary protection, and the regulation of commercial space activities. Furthermore, exploring the economic opportunities and challenges associated with space colonization, such as asteroid mining and space tourism, will be essential for understanding the potential impact on global markets and human society.

REFERENCES

[1] "Elon Musk on SpaceX's Reusable Rocket Plans". 7 February 2012. Archived from the original on 24 June 2017. Retrieved 13 June 2015.
[2] Jump up to:a b Britt, Robert Roy (8 October 2001). "Stephen Hawking: Humanity Must Colonize Space to Survive". space.com. Archived from the original on 25 November 2010. Retrieved 2006- 07-28.
[3] "Japan vs. NASA in the Next Quantum Cryptography run : Lunar Robonauts". Fast Company. 28 May 2010. Retrieved 12 June 2015.
[4] "SOLAR SYSTEM EXPLORATION RESEARCH". Retrieved 11 August 2017.
[5] Mike Wall (25 October 2019). "Bill Nye: It's Space Settlement, Not Colonization". Space.com. Retrieved 26 November 2020.
[6] Bartels, Meghan (May 25, 2018). "People are calling for a movement to decolonize space-here's why". Newsweek. Retrieved Oct 31, 2021. Robert Zubrin, said that the one word he shies away from is colony, preferring settlement because the first "confuses the issue with imperialism."