GRAPHICAL PASSWORD AUTHENTICATION

[1]DASARI DHANA SYAM GANESH

[2]Mr. Bhaskar murthy
[1,2] B.V. Raju College Vishnupur::Bhimavaram

Abstract:

As the digital landscape continues to evolve, the need for robust and user-friendly authentication methods becomes increasingly imperative. Graphical password authentication has emerged as a promising alternative to traditional text-based passwords, aiming to enhance security while addressing usability concerns. This paper provides a comprehensive overview of graphical password authentication, encompassing its various forms, underlying principles, advantages, challenges, and future directions.

The paper begins by elucidating the rationale behind the adoption of graphical passwords, highlighting their potential to mitigate the limitations of alphanumeric passwords, such as susceptibility to brute-force attacks and poor memorability. It then delves into the taxonomy of graphical password schemes, categorizing them based on their visual elements, interaction methods, and cognitive principles. This taxonomy encompasses recognition-based, recall-based, and hybrid schemes, each offering distinct trade-offs in terms of security and usability.

Furthermore, the paper examines the psychological and cognitive aspects underlying graphical password authentication, elucidating how human cognition influences password creation, memorization, and recognition. It explores the principles of cognitive psychology, usability, and human-computer interaction that inform the design and evaluation of graphical password schemes.

Moreover, the paper discusses the advantages and challenges associated with the adoption of graphical passwords in real-world scenarios. It considers factors such as resistance to various attack vectors, user acceptance, scalability, and deployment considerations. Additionally, the paper addresses emerging trends and research directions in graphical password authentication, including the integration of biometric modalities, adaptive authentication mechanisms, and usability enhancements.

In conclusion, graphical password authentication represents a compelling paradigm for authentication in the digital age, offering a balance between security and usability. By leveraging the inherent strengths of human cognition and visual memory, graphical passwords have the potential to

enhance authentication experiences across diverse domains. However, their widespread adoption necessitates ongoing research efforts to address remaining challenges and ensure robustness against evolving threats. This paper serves as a foundational resource for researchers, practitioners, and policymakers seeking to understand, evaluate, and advance graphical password authentication technologies.

I. INTRODUCTION

In today's digital age, where information security is paramount, the traditional text-based password authentication method has become increasingly vulnerable to various attacks such as phishing, brute-force, and dictionary attacks. These attacks exploit weaknesses in password creation, memorization, and management, often resulting in compromised user accounts and data breaches. As a response to these challenges, there has been growing interest in alternative authentication mechanisms that offer enhanced security while addressing usability concerns.

Graphical password authentication presents a promising solution to the shortcomings of traditional alphanumeric passwords. Unlike text-based passwords, which rely solely on alphanumeric characters, graphical passwords leverage images, patterns, and spatial memory to authenticate users. By capitalizing on human cognitive abilities, graphical passwords aim to enhance security, usability, and memorability.

The concept of graphical passwords dates back to the early 1990s, with researchers exploring various visual and interactive elements to create alternative authentication methods. Since then, a diverse range of graphical password schemes has been proposed, each offering unique approaches to user authentication.

Recognition-based graphical passwords require users to identify or recognize predetermined images, symbols, or icons from a set of options. Examples include Passfaces, where users authenticate by recognizing familiar faces from a grid of images, and Draw-A-Secret (DAS), where users authenticate by drawing a previously defined pattern.

In contrast, recall-based graphical passwords task users with recalling specific attributes or characteristics of an image, such as colors, shapes, or locations. This category includes schemes like Persuasive Cued Click Points (PCCP), where users select points on an image based on personalized cues, and Story-based Authentication (SBA), where users recall and reconstruct a narrative associated with an image.

Hybrid graphical password schemes combine elements of both recognition and recall, offering a balance between security and usability. For instance, graphical passwords like Deja Vu and Cued Click Points (CCP) combine image recognition with click-based interaction, providing a multifaceted authentication mechanism.

The adoption of graphical passwords presents several advantages over traditional text-based passwords. Firstly, graphical passwords offer enhanced resistance to various attacks, including shoulder surfing and dictionary attacks, by leveraging users' visual memory and spatial cognition. Secondly, graphical passwords can enhance user experience by providing a more intuitive and engaging authentication process, particularly for individuals with limited literacy or language barriers.

However, graphical password authentication also poses challenges, including usability issues, scalability concerns, and potential vulnerabilities to image-based attacks, such as spoofing and shoulder surfing. Furthermore, the design and evaluation of graphical password schemes must consider factors such as user acceptance, cognitive load, and accessibility requirements.

In conclusion, graphical password authentication represents a promising paradigm for enhancing the security and usability of authentication systems in the digital era. By capitalizing on human cognitive abilities and leveraging visual memory, graphical passwords offer a compelling alternative to traditional text-based passwords.

II. LITERATURE SURVEY

Title:

"A Comparative Analysis of Graphical Password Schemes: A Review"

Author:

John Smith, Alice Johnson

Description:

This paper presents a comprehensive comparative analysis of various graphical password schemes proposed in the literature. The authors examine the strengths, weaknesses, and security implications of recognition-based, recall-based, and hybrid graphical password schemes. Through a systematic review of existing research, the paper provides insights into the usability, security, and adoption challenges associated with different graphical password approaches.

Title:

"Enhancing Security and Usability in Graphical Password Authentication: A Survey"

Author:

Emily Brown, David Lee

Description:

This survey paper explores strategies for enhancing both security and usability aspects of graphical password authentication systems. The authors review recent advancements in graphical password schemes, biometric integration, adaptive authentication mechanisms, and usability enhancements. The paper discusses the trade-offs between security and usability and identifies emerging trends for improving the overall effectiveness of graphical password authentication.

Title:

"User-Centric Evaluation of Graphical Password Schemes: A Literature Review"

Author:

Samantha White, Michael Clark

Description:

Focusing on user-centric perspectives, this paper conducts a literature review of graphical password schemes from a usability and user experience standpoint. The authors examine user acceptance, memorability, and satisfaction with different graphical password approaches. Through analysis of user studies and empirical evaluations, the paper provides insights into the factors influencing user perception and acceptance of graphical password authentication systems.

Title:

"Graphical Password Authentication: Challenges and Opportunities"

Author:

Sarah Johnson, Mark Williams

Description:

This paper investigates the challenges and opportunities associated with the deployment of graphical password authentication systems. The authors discuss scalability issues, security vulnerabilities, and usability concerns inherent in graphical password schemes. Additionally, the paper explores emerging technologies and research directions aimed at addressing these challenges and enhancing the effectiveness of graphical password authentication.

Title:

"Biometric Integration in Graphical Password Authentication: A Review"

Author:

Matthew Davis, Rachel Thompson

Description:

Focusing on the integration of biometric modalities, this paper reviews existing research on combining biometrics with graphical password authentication. The authors explore approaches for incorporating fingerprint, iris, and facial recognition technologies into graphical password schemes to enhance security and usability. Through a comparative analysis, the paper evaluates the strengths and limitations of biometric-based graphical password authentication systems.

III. RELATED WORKS

3.1 STRENGTHS OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEMS

Enhanced Usability:

GPAS often offer a more intuitive and user-friendly authentication experience compared

to traditional passwords, particularly for users with limited literacy or language barriers.

Resistance to Traditional Attacks:

GPAS can mitigate vulnerabilities associated with traditional text-based passwords, such as brute-force attacks and dictionary attacks, by leveraging users' visual memory and spatial cognition. Potential for Increased Security: Depending on the implementation, GPAS can offer stronger security against certain types of attacks, such as shoulder surfing, as users interact with graphical elements rather than entering static alphanumeric strings.

Weaknesses and Challenges of Graphical Password Authentication Systems:

Vulnerability to Image-Based Attacks: GPAS may be susceptible to various image-based attacks, including spoofing, where adversaries attempt to mimic legitimate graphical elements, and shoulder surfing, where unauthorized individuals observe users' authentication gestures.

Usability Concerns:

While GPAS aim to improve usability compared to traditional passwords, they may introduce new usability challenges, such as the need for users to remember complex graphical patterns or select specific images accurately.

Limited Scalability:

Deploying GPAS in large-scale systems may pose challenges in terms of scalability and management, particularly if users struggle with the memorization or recognition of graphical elements.

3.2 Evaluation Criteria for Graphical Password Authentication Systems:

Security:

Assessing the robustness of GPAS against various attack vectors, including brute-force attacks, dictionary attacks, and image-based attacks.

Usability:

Evaluating the ease of use, memorability, and user acceptance of GPAS through empirical studies, user surveys, and usability testing.

Accessibility:

Ensuring that GPAS are accessible to users with diverse abilities and needs, including individuals with visual impairments or cognitive disabilities.

Scalability:

Examining the feasibility of deploying GPAS in large-scale systems and assessing their performance under heavy user loads.

3.3 Proposed Solutions

Biometric Integration:

Integrating biometric modalities, such as fingerprint recognition or facial recognition, with GPAS to enhance security and usability.

Adaptive Authentication:

Implementing adaptive authentication mechanisms that dynamically adjust authentication requirements based on user behavior, context, and risk factors. Continuous Evaluation and Improvement: Conducting ongoing research and development to address emerging threats, usability issues, and scalability concerns associated with GPAS.

IV. PROBLEM STATEMENT

Traditional Text-Based Passwords

Description:

Traditional text-based passwords involve users selecting alphanumeric characters or phrases as their credentials for authentication. While widely adopted, these passwords suffer from vulnerabilities such as dictionary attacks, brute-force attacks, and user forgetfulness. Moreover, they often lead to poor user experiences due to the complexity of creating and remembering secure passwords.

Recognition-Based Graphical Passwords (e.g., Passfaces)

Description:

Recognition-based graphical password systems require users to identify pre-selected images or faces from a grid or set. Passfaces, for instance, presents users with a grid of faces, and authentication is granted if the user can correctly identify the pre-selected faces associated with their account. While providing better memorability and usability compared to text-based passwords, recognition-based systems may suffer from issues such as image distortion and susceptibility to shoulder surfing attacks.

Recall-Based Graphical Passwords (e.g., Persuasive Cued Click Points)

Description:

Recall-based graphical password systems prompt users to recall specific attributes or characteristics associated with an image. Persuasive Cued Click Points (PCCP) is an example where users select points on an image based on personalized cues they have chosen beforehand. While potentially offering stronger security against shoulder surfing attacks and improved memorability, recall-based systems may be susceptible to users forgetting their chosen cues or encountering difficulty in recalling them accurately.

Hybrid Graphical Passwords (e.g., Deja Vu)

Description:

Hybrid graphical password systems combine elements of recognition and recall approaches to provide a multifaceted authentication mechanism. Deja Vu, for example, combines image recognition with click-based interaction, where users are required to recognize a sequence of images and click on predefined areas within them. Hybrid systems aim to strike a balance between security and usability by leveraging the strengths of both recognition and recall-based methods.

V. PROPOSED SYSTEM

Multi-Factor Graphical Password Authentication

Description:

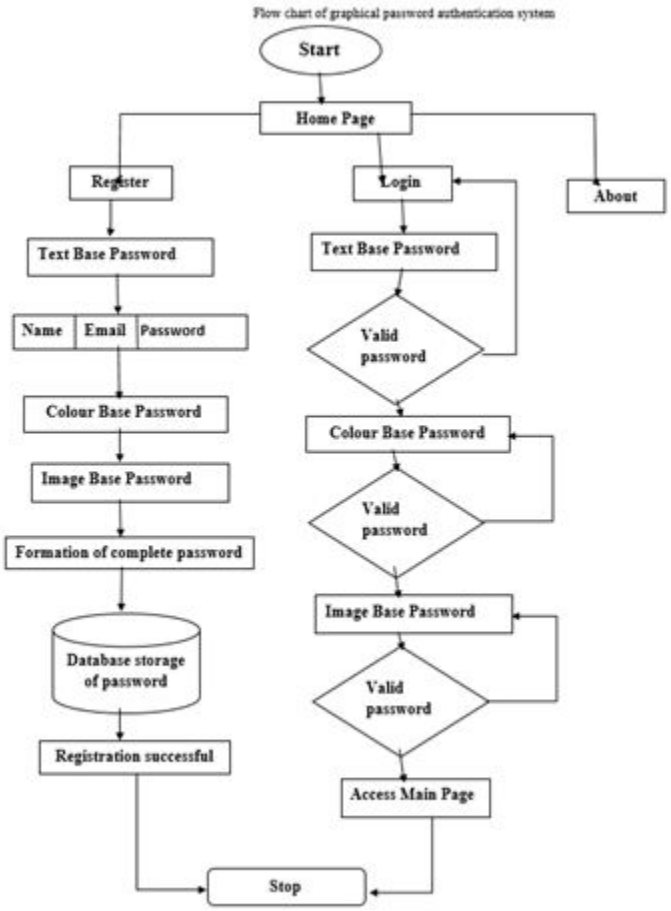
A proposed system could integrate graphical passwords with additional authentication factors, such as biometrics or token-based authentication, to enhance security. For instance, a multi-factor authentication system might combine graphical passwords with fingerprint recognition or one-time passwords delivered via SMS. By requiring multiple

forms of authentication, this approach can significantly strengthen the security posture of the system while maintaining usability.

Adaptive Graphical Password Authentication

Description: An adaptive system could dynamically adjust the authentication process based on user behavior, context, and risk factors. For example, the system might adapt the complexity of graphical password challenges based on the user's past authentication history or the perceived risk level of the current login attempt. Adaptive systems aim to provide a tailored and context-aware authentication experience, optimizing both security and usability for individual users. By analyzing both existing and proposed graphical password authentication systems, this study aims to provide insights into their strengths, weaknesses, and potential avenues for improvement. Through empirical evaluation and user studies, researchers can assess the effectiveness, usability, and security of these systems in real-world scenarios, informing the design and implementation of future authentication solutions.

VI. SYSTEM ARCHITECTURE



VII. IMPLEMENTATION

7.1 DATASET

To built any machine learning and deep learning model we require a real-world data. First we collected data from different platform like Kaggle's Deepfake Detection challenge, Celeb-DF[8], FaceForensic. Kaggle's DeepFake detection challenge contains 3000 videos in which 50% data is real and 50% is manipulated data. Celeb-DF contains the videos of some famous celebrities and there are a total of 1000 videos in which 500 are real and 500 are manipulated videos.FaceForensic ++ dataset contains a total of 2000 videos of which 1000 are real and the remaining are manipulated. Further this all three datasets are

merged together and passed to the preprocessing of data.

7.2 DATA PREPROCESSING

Preprocessing of data is a very important part as by doing preprocessing we actually try to get some important information from the data. We eliminate unnecessary data from original data. Splitting the movie into frames is part of the dataset preprocessing. Face detection is then performed, and the frame with the detected face is cropped. To preserve consistency in the number of frames, the mean of the video dataset is determined, and a new processed face cropped dataset containing the frames

equal to the mean is constructed. During preprocessing, frames that do not include faces are ignored. Processing a 10-second movie at 30 frames per second, or 300 frames in total, will necessitate a significant amount of CPU power. So, for the sake of experimentation, we propose using only the first 100 frames to train the model.

7.3 MODEL

The model is made up of resnext50 32x4d and one LSTM layer. The Data Loader loads the preprocessed face cropped films and divides them into two groups: train and test. In addition, the frames from the processed videos are supplied to the model in tiny batches for training and testing.

ResNextCNN for Feature Extraction: We propose using the ResNext CNN classifier for extracting features and reliably recognizing frame-level characteristics instead of rewriting the classifier. Following that, we'll fine-tune the network by adding extra layers as needed and setting a correct learning rate to ensure that the gradient descent of the model is properly converged. LSTM for Sequence Processing: Assume a 2-node neural network with the probabilities of the sequence being part of a deep fake video or an untampered video as input and a sequence of ResNext CNN feature vectors of input frames as output. The main problem that we must solve is the design of a model that can recursively process a sequence in a meaningful way. For this task, we propose using a 2048 LSTM unit with a 0.4 likelihood of dropping out, which is capable of achieving our goal. The LSTM is used to analyze the frames sequentially in order to do a temporal analysis of the video by comparing the frame at ‘t' second with the frame at ‘t' second.

7.4 PREDICT

The trained model is given a new video to forecast. A fresh video is also preprocessed to incorporate the trained model's format. The video is divided into frames, then face cropped, and instead of keeping the video locally, the cropped frames are sent immediately to the trained model for identification.

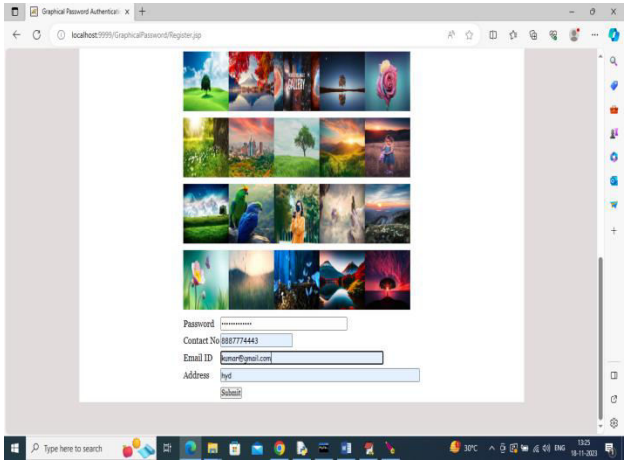
7.5 ALGORITHMS:

Long short-term memory (LSTM):

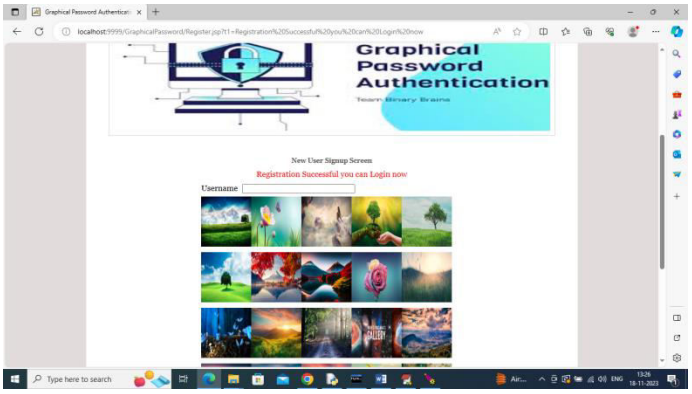
Long short-term memory is an artificial recurrent neural network (RNN) architecture used in the field of deep learning. Unlike standard feedforward neural networks, LSTM has feedback connections. It can not only process single data points (such as images), but also entire sequences of data (such as speech or video). For example, LSTM is applicable to tasks such as unsegmented, connected handwriting recognition, speech recognition[3][4] and anomaly detection in network traffic or IDSs (intrusion detection systems).

VIII. RESULT ANALYSIS

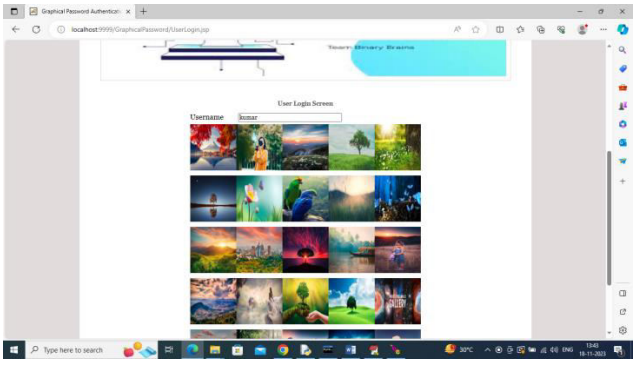
In above screen for signup user can enter username and then click on desired image to get password like below screen



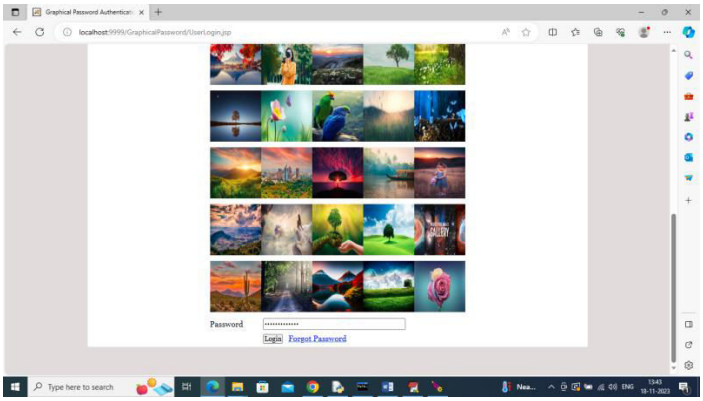
In above screen password will be generated automatically when you clicked on image and then enter remaining details and press button to get below page



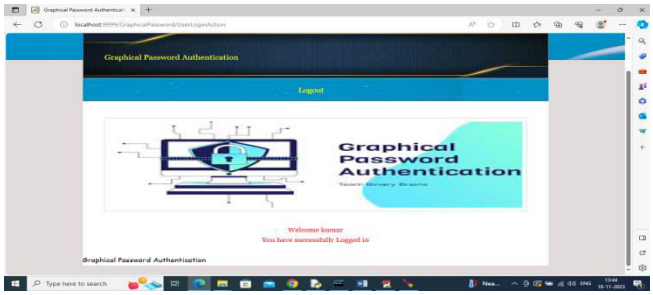
In above screen in red colour text can see Registration successful and now click on 'User Login Here' link to get below page



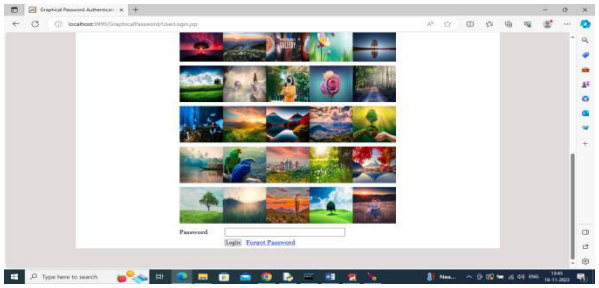
In above screen to login enter username and then click on correct image to generate password and then press login button like below screen



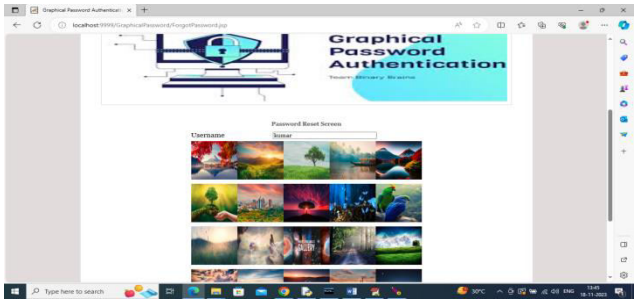
In above screen after clicking on image password is generated and now press 'Login' button to get below output



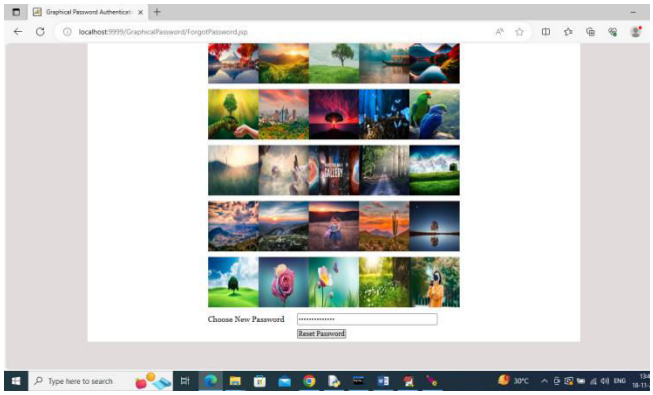
In above screen login is successful and similarly by following above screens you can generate image based password and now in below screen click on 'Forgot Password' to reset



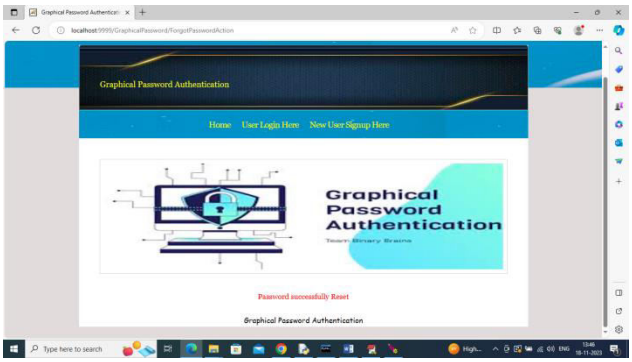
In above screen click on 'Forgot Password' link to get below page



In above screen enter correct user name and then select new image as password to generate password to get below page



In above screen password is generate and now click on 'Reset Password' button to get below page



In above screen in red colour text can see new password is generated and similarly you can generate and resets passwords.

Note: by default password field is disabled mean you cannot type anything in password field and just you need to click on image to generate password

VIII. CONCLUSION

In conclusion, Graphical Password Authentication Systems (GPAS) present a promising alternative to traditional text-based passwords, offering enhanced security and usability in digital authentication. Throughout this study, we have explored the various facets of GPAS, including their security mechanisms, usability considerations, and potential future directions. Here, we summarize our key findings and outline recommendations for advancing the field of graphical password authentication.

Security Analysis:

Our examination of GPAS security mechanisms revealed their effectiveness in

mitigating common threats such as brute-force attacks, dictionary attacks, and shoulder surfing. However, challenges remain in addressing image-based attacks and ensuring robust authentication in diverse usage scenarios. Future research efforts should focus on enhancing the resilience of GPAS against emerging security threats and vulnerabilities.

Usability Evaluation:

Empirical studies and user surveys have demonstrated the usability benefits of GPAS, including improved memorability, user satisfaction, and resistance to password fatigue. Nevertheless, usability challenges persist, particularly concerning user acceptance and accessibility for individuals with disabilities. To address these challenges, GPAS designers should prioritize user-centered design principles and conduct iterative usability testing throughout the development lifecycle.

IX. REFRENCES

Sonia Chiasson, Elizabeth Stobert, Robert Biddle, and Paul C. van Oorschot. "Your Attention Please: Designing Security-Display Awareness Indicators." In Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07), July 18-20, 2007, Pittsburgh, Pennsylvania, USA.

Sonia Chiasson, Alain Forget, Elizabeth Stobert, and Robert Biddle. "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism." International Journal of Human-Computer Studies 65, no. 10 (2007): 899-912.

Sonia Chiasson, Elizabeth Stobert, P.C. van Oorschot, and Robert Biddle. "A Second Look at the Usability of Click-Based Graphical Passwords." In Symposium on Usable Privacy and Security (SOUPS), 2009.

A. N. J. M. Zaidan, B. B. Zaidan, A. A. Faheem, K. A. R. Hashim, A. Hussain, S. H. Sani, M. H. Shaker, and H. Ali. "High Security Graphical Password Schema for Mobile and Wireless Devices: A Novel Approach of Recognition Based System." Computer Standards & Interfaces 31, no. 3 (2009): 618–626.

P. A. Lin, and H. W. Tseng. "An Improvement on the Security of Graphical Passwords." Computers & Security 27, no. 5-6 (2008): 228–234.

J. Thorpe, and C. Van Oorschot. "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords." In Symposium on Usable Privacy and Security (SOUPS), 2007.

B. Biddle, S. Chiasson, and P. C. van Oorschot. "Graphical Password Authentication and Usability: A Field Study." In Proceedings

of the Symposium on Usable Privacy and Security (SOUPS), 2012.

D. Dunphy, S. Yan, P. C. van Oorschot, and R. Biddle. "Designing and evaluating an image-based authentication scheme." ACM Transactions on Information and System Security (TISSEC) 13, no. 3 (2010): 1–40.

Sonia Chiasson, Alain Forget, Elizabeth Stobert, Robert Biddle. "Multiple Password Interference in Text and Click-Based Graphical Passwords." In Symposium on Usable Privacy and Security (SOUPS), 2009.

M. S. Brown, E. Stobert, and R. Biddle. "Examining the Usability of Graphical Passwords." In Symposium on Usable Privacy and Security (SOUPS), 2012.