ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

https://doi.org/10.5281/zenodo.14351064

Provision Of Web Security Using Graphical Passwords

Rasoju Prashanthi[1], Dr. B. Narsimha[2]

[1]PG Scholar, Department of CSE, Teegala Krishna Reddy Engineering College (Autonomous Institution),Medbowli, Meerpet, Saroornagar,Hyderabad

[2]Professor, Department of CSE, TeegalaKrishnaReddyEngineeringCollege (Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad

ABSTRACT

The proposed project is a Provision of Web Security Using Graphical Passwords that utilizes Python Flask for the backend, HTML/CSS for the frontend, and JavaScript for user interactions. The system allows users to upload an image, which is then divided into a 3x3 grid of segments. Each segment is assigned a password input field, and the user must enter a password in at least three of the nine image segments to create a password.The user's information and passwords are stored in a secure database, ensuring the system's security.The system is developed using Python Flask for the server-side programming, HTML/CSS for the user interface design, and JavaScript for user interactions. The system's usability and security are tested, and its performance is evaluated based on accuracy, efficiency, and user satisfaction.Overall, the graphical password authentication system provides a secure and user-friendly alternative to traditional alphanumeric password-based authentication systems. The system can be integrated into various applications to improve user authentication and security. The use of Python Flask, HTML/CSS, and JavaScript provides a flexible and robust platform for developing this graphical password authentication system.

Keywords:Flask,Web Security,HTTPS,Distributed Denial of Service

I. INTRODUCTION

In today's digital age, ensuring the security of online accounts and data has become more critical than ever before. One way to enhance web security is by using graphical passwords. Unlike traditional text-based passwords, graphical passwords allow users to select images, shapes, or patterns to secure their accounts. This approach can be more secure because it is harder to guess or crack a graphical password, especially if the images used are unique to the user and not easily guessable. Web security is an essential aspect of the digital world, as it ensures the protection of sensitive information and prevents unauthorized access to web applications. Traditional methods of web security, such as alphanumeric passwords, are often vulnerable to attacks like brute force and dictionary attacks. In recent years, graphical passwords have emerged as a promising alternative for enhancing web security. Unlike

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

alphanumeric passwords, graphical passwords allow users to choose a combination of images, symbols, and gestures to create a unique password. This approach offers several advantages, such as improved memorability, reduced susceptibility to guessing attacks, and increased resistance to shoulder surfing. Additionally, graphical passwords are more user-friendly and accessible to individuals with disabilities, such as dyslexia or blindness. This paper explores the provision of web security using graphical passwords, highlighting the benefits and drawbacks of this approach. The study also provides an overview of different graphical password schemes and their effectiveness in enhancing web security. Ultimately, the goal is to offer insights into how graphical passwords can be effectively integrated into web security systems to enhance protection and prevent unauthorized access. In this context, this essay aims to explore the use of graphical passwords as a means of improving web security. It will discuss the advantages and disadvantages of graphical passwords and provide an overview of the current state of research in the field. Ultimately, the goal is to highlight the potential of graphical passwords as an effective and user-friendly approach to web security.

II. RELATED WORK

Cyber-criminals have benefited from on-line banking (OB), regardless of the extensive research on financial cyber-security. To better be prepared for what the future might bring, to predict how hacking tools might evolve. Briefly survey the state-of-the-art tools developed by black-hat hackers and conclude that automation is starting to take place. To demonstrate the feasibility of our predictions and prove that many two-factor authentication schemes can be bypassed, developed three browser rootkits which perform the automated attack on the client's computer. Also, in some banks attempt to be regarded as user-friendly, security has been downgraded, making them vulnerable to exploitation.

Two factor confirmation utilizing cell phones. The proposed technique ensures that validating to administrations, for example, internet managing an account or ATM machines, is done in extremely secure way. The proposed framework includes utilizing a cell phone as a product token for One Time Password age. The created One Time Password is substantial for just a short client characterized timeframe and is produced by factors that are extraordinary to both, the client and the cell phone itself. Moreover, a SMS-based component is executed as both a reinforcement system for recovering the watchword and as a conceivable mean of

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

synchronization. Presents another security rough in light of hard AI issues, specifically, a novel gathering of graphical mystery key structures based over Puzzle technology, which call Puzzle as graphical passwords (DSA). Captcha is both a Puzzle and a graphical mystery key arrangement. Captcha keeps an eye on different security issues completely, for instance, electronic guessing ambushes, exchange attacks, and, if joined with dual see progressions, bear surfing strikes. Prominently, a Captcha mystery key can be found just probabilistically by means of customized online hypothesizing attacks paying little heed to whether the watchword is in the request set. Captcha in like manner offers a novel method to manage address the picture hotspot issue in understood graphical mystery key systems, for instance, Pass Points, that every now and again prompts delicate watchword choices. Captcha isn't a panacea, yet it offers sensible security and convenience and appears to fit well with some utilitarian applications for improving on the web security. Present excellent Captcha in view of both substance Puzzle and picture affirmation Puzzle. One of them is a substance Captcha wherein a mystery word is a gathering of characters like a substance watchword, however entered by tapping the right character progression on Captcha pictures. Captcha offers protection against online vocabulary attacks on passwords.

Protection against online lexicon assaults is a more unpretentious issue than it may appear. Puzzle Login(top of Puzzle innovation Using numerical problems).Image Puzzle Solving Using AES Algorithm. In this section, we propose a secure user authentication protocol, which describe a remote user authentication with Mobile Token, shoulder-surfing resistant graphical password and a SPGA algorithm which generates a strong password.

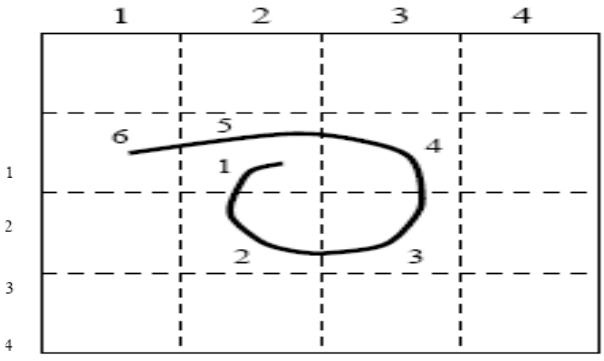
S. Wiedenbeck et al [7], have invented the pass point system for password authentication. The concept of the pass point was as simple as just clicking five point on single image and combination of this point as a password. In this system user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. But the main security problem with this was the HOTSPOT, the area where the user clicks.

A system proposed by Syukri and colleagues, the authentication is done by drawing a signature with the mouse in this system. Online signature recognition is another topic and it will not be discussed more in this paper.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
https://doi.org/10.5281/zenodo.14351064
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024

By using Syukri and his colleagues system, it is easy to remember the passwords and difficult to use by others because it allows users to use their own signature as a password. However, it has the disadvantages of being difficult to use and the procedure of recognition is complicated. In recent years, the techniques that use graphical passwords and text-based passwords together also had been introduced [16]. Chapter 3, a new concept graphical password system called PassPositions.

Jermyn and his colleagues introduce a system known as DAS (Draw-A-Secret) as recall-based Graphical Passwords. This system is a system that can draw a pattern shown as below.



In the DAS system, there are divided areas on the screen, and a pattern is drawn as they pass through the areas. As the pattern is drawn the order of the passing area is remembered, and the passing order of the areas should be the same for authentication. Therefore, the user should memorize the pattern and reproduce it at the time of authentication.

The cracking process is done by using software named Cain & Abel. Cain & Abel allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords and more. This software uses Brute Force technique which tries every combination of ASCII character based on try and error methods that used by application programs to decode encrypted data in order to gain information such as username and passwords. However, the tools were not able to crack the proposed image-based passwords because all the password cracking tools and technique is not be able to crack image-based passwords. Even if attacker tries to network sniff the password, they are not being able to crack it because the passwords stored for this study is already being hashed and it is not in a plain text.

III.IMPLEMENTATION

Web security using graphical passwords typically involves using images or symbols as a means of authentication instead of traditional text-based passwords.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

Image selection: The user is presented with a set of images or symbols from which they choose a specific image or a combination of images as their password. The selection process can be random or pre-determined by the system.

Password creation: After selecting their images, the user needs to create a password by placing the images in a specific order, sequence or position. This creates a unique combination of images that serves as their password.

Password verification: When the user logs in, they need to provide their graphical password by selecting the images in the same order or position as they did during password creation. The system then verifies the password for accuracy.

Randomization: The system can randomize the images presented to the user each time they log in to prevent pattern recognition and guessing attacks.

Error handling: The system should provide clear error messages to the user if they enter their password incorrectly, such as indicating which image was selected incorrectly or providing suggestions for password recovery.

Security measures: The system should have robust security measures in place to protect against various types of attacks, such as brute-force attacks, phishing attacks, and shoulder-surfing attacks.

Usability: The system should be designed with the user in mind, providing a user-friendly interface, clear instructions, and easy password recovery options.

Overall, the key functions for provision of web security using graphical passwords are similar to those for traditional alphanumeric passwords, with a few key differences related to image selection and password creation. By implementing these functions effectively, graphical passwords can provide an additional layer of security for web applications.

IV.ALGORITHM

Network Security

Network security refers to the measures taken to protect computer networks from unauthorized access, use, modification, or destruction. It includes both hardware and software technologies, as well as policies and procedures designed to ensure the security of the network and its data.

Web security

Web security refers to the measures taken to protect websites, web applications, and web services from unauthorized access, use, modification, or destruction. With the increasing prevalence of online activities and e-commerce, web security has become critical to protecting sensitive information

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

such as personal data, financial information, and intellectual property.

HTTPS is a protocol that encrypts communication between a website and its users. It is essential for protecting sensitive data such as passwords, credit card information, and personal details. Regularly updating software is important for fixing vulnerabilities and preventing attacks. This includes not only the website's code but also any third-party software, such as content management systems, plugins, and frameworks. Access controls limit access to specific resources and data within a web application. This includes authentication, authorization, and role-based access control. Firewalls can help block unauthorized access to a website and prevent attacks such as Distributed Denial of Service (DDoS).Regular security testing, including vulnerability scanning and penetration testing, can help identify weaknesses in a web application and allow for remediation before an attacker can exploit them.

Flask Framework:

Flask is a lightweight WSGI web application framework. It is designed to make getting started quick and easy, with the ability to scale up to complex applications. It began as a simple wrapper around Werkzeug and Jinja and has become one of the most popular Python web application frameworks.

Flask offers suggestions, but doesn't enforce any dependencies or project layout. It is up to the developer to choose the tools and libraries they want to use. There are many extensions provided by the community that make adding new functionality easy.

```
from flask import Flask, escape, request
app = Flask(__name__)
@app.route('/')
def hello():
name = request.args.get("name", "World")
return f'Hello, {escape(name)}!'
$ env FLASK_APP=hello.py flask run
* Serving Flask app "hello"
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
```

Flask is a micro web framework written in Python. It is classified as a microframework because it does not require particular tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions. However, Flask supports extensions that can add application features as if they were implemented in Flask itself. Extensions exist for object-relational mappers, form validation, upload handling, various open authentication technologies and several common framework related tools.

Applications that use the Flask framework include Pinterest and LinkedIn.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

V. RESULTS

Fig:1 Login page

Fig:2 Signup Page

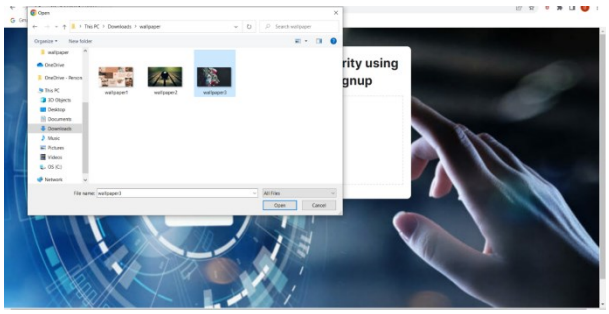


Fig:3 Upload Page

Fig:4.Verification Page

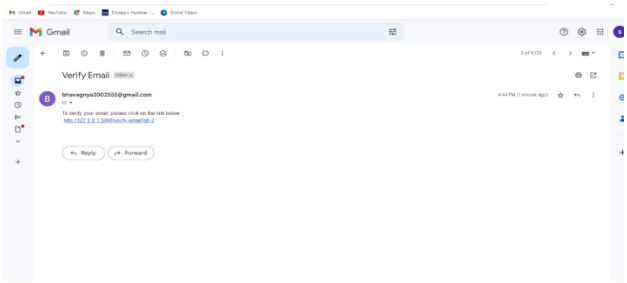


Fig:5.Verification

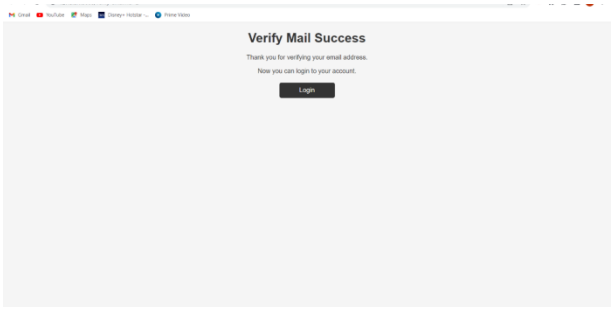


Fig:6.Verify Mail

Fig:7.Web security of Graphical Passwords

8. CONCLUSION

In conclusion, graphical passwords can provide an additional layer of security for web applications. By using images instead of text-based passwords, graphical passwords are less vulnerable to attacks such as brute force and dictionary attacks. However, the effectiveness of graphical passwords depends on

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

the design of the graphical password system and user behavior.

To ensure the provision of web security using graphical passwords, the system must have a strong and secure encryption algorithm, and an effective method for storing passwords. Additionally, users must be educated on best practices for creating and storing their graphical passwords, such as using complex images and avoiding common patterns or themes.

At last the graphical passwords can provide an alternative method for securing web applications, they should be used in combination with other security measures, such as two-factor authentication and regular password updates, to ensure maximum protection against cyber threats.

REFERENCES:

1. Priya, K.; Venkaiah Naidu, T.; Vamsi Krishna, R. (2018). [IEEE 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) - Tirunelveli, India (2018.5.11-2018.5.12)] 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) - An Advanced Information Security System Using Image Based Graphical Password Scheme. , (), 304–307.

2.Kolekar, Vikas K.; Vaidya, Milindkumar B. (2015). [IEEE 2015 International Conference on Information Processing (ICIP) - Pune, India (2015.12.16-2015.12.19)] 2015 International Conference on Information Processing (ICIP) - Click and session based — Captcha as graphical password authentication schemes for smart phone and web. , (), 669–674

3.Ma, Yao; Feng, Jinjuan (2011). [IEEE 2011 9th International Conference on Software Engineering Research, Management and Applications (SERA) - Baltimore, MD, USA (2011.08.10-2011.08.12)] 2011 Ninth International Conference on Software Engineering Research, Management and Applications - Evaluating Usability of Three Authentication Methods in Web-Based Application. , (), 81–88

4. Bhand, Amol; Desale, Vaibhav; Shirke, Swati; Shirke, Suvarna Pansambal (2015). [IEEE 2015 International Conference on Information Processing (ICIP) - Pune, India (2015.12.16-2015.12.19)] 2015 International Conference on Information Processing (ICIP) - Enhancement of password authentication system using graphical images. , (), 217–219.

5.Eljetlawi, Ali Mohamed; Ithnin, Norafida (2008). [IEEE 2008 Third International Conference on Convergence and Hybrid Information Technology (ICCIT) - Busan, Korea (2008.11.11-2008.11.13)] 2008 Third International Conference on Convergence and Hybrid Information Technology - Graphical Password: Comprehensive

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

Study of the Usability Features of the Recognition Base Graphical Password Methods. , (), 1137–1143

6.Lupu, Viorel (2018). [IEEE 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) - Stuttgart, Germany (2018.6.17-2018.6.20)] 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) - Securing Web Accounts by Graphical Password and Voice Notification. , (), 1–5.

7.Shen, Sung-Shiou; Kang, Tsai-Hua; Lin, Shen-Ho; Chien, Wei (2017). [IEEE 2017 International Conference on Applied System Innovation (ICASI) - Sapporo, Japan (2017.5.13-2017.5.17)] 2017 International Conference on Applied System Innovation (ICASI) - Random graphic user password authentication scheme in mobile devices. , (), 1251–1254

8.Prakash, Sreya; Sreelakshmy, M. K. (2017). Eljetlawi, Ali Mohamed; Ithnin, Norafida (2008). [IEEE 2008 Third International Conference on Convergence and Hybrid Information Technology (ICCIT) - Busan, Korea (2008.11.11-2008.11.13)] 2008 Third International Conference on Convergence and Hybrid Information Technology - Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods. , (), 1137–1143.

9.Jiang, Ming; He, Ai; Wang, Kuangyu; Le, Zhengyi (2015). [IEEE 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud) - New York, NY, USA (2015.11.3-2015.11.5)] 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing - Two-Way Graphic Password for Mobile User Authentication(),476–481.

10.Varshney, Gaurav; Misra, Manoj; Atrey, Pradeep (2017). [IEEE 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID) - Xiamen, China, China (2017.10.27-2017.10.29)] 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID) - A new secure authentication scheme for web login using BLE smart devices. , (), 95–98

11.Zujevs, Nikita (2019). [IEEE 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE) - London, United Kingdom (2019.8.22-2019.8.23)] 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE) - Authentication by Graphical Passwords Method ‘Hope’. , (), 94–99.

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 4, 2024
https://doi.org/10.5281/zenodo.14351064

12.Yang, Gi-Chul (2017). [IEEE 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) - Kuta Bali, Indonesia (2017.8.8-2017.8.10)] 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) - PassPositions: A secure and user-friendly graphical password scheme. , (), 1–5.

13.Janakiraman, Siva; Sri, V S Karunya; Pulluri, Chathurya; Rajagopalan, Sundararaman; Thenmozhi, K; Rengarajan, (2017). [IEEE 2017 International Conference on Computer Communication and Informatics (ICCCI) - Coimbatore, India (2017.1.5-2017.1.7)] 2017 International Conference on Computer Communication and Informatics (ICCCI) - Numerical password via graphical input — An authentication system on embedded platform. , (), 1–5.

14.Jaffar Abduljalil Jaffar;Ahmed M. Zeki; (2020). Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability . 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), (), –

15.Othman, Noor Ashitah Abu; Rahman, Muhammad Akmal Abdul; Sani, Anis Shobirin Abdullah; Ali, Fakariah Hani Mohd (2018). [IEEE 2018 IEEE Conference on Systems, Process and Control (ICSPC) - Melaka, Malaysia (2018.12.14-2018.12.15)] 2018 IEEE Conference on Systems, Process and Control (ICSPC) - Directional Based Graphical Authentication Method with Shoulder Surfing Resistant. , (), 198–202