Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

System Authentication System

[1] Syed Mahboob, [2] Syed Suwaid Ullah Hussaini, [3] Mr. Mohammed Rahmat Ali
[1] BE Student, Dept. of Computer Science Engineering, ISL Engineering College
[2] BE Student, Dept. of Computer Science Engineering, ISL Engineering College
[3] Assistant Professor, Dept. of Computer Science Engineering, ISL Engineering College

Article Info
Page Number: 1587 - 1593
Publication Issue:
Vol 72 No. 1 (2023)

Abstract

A graphical password secure authentication system is one of technic for authentication of computer security. Today, computer science's most crucial component for protecting user or client data is digital/computer security. And one of the hazards is shoulder-surfing, in which a thief might obtain a password by keeping watch on the authentication process or filming it. There are several approaches for this authentication, with the Graphical Password Technique being the most popular and straightforward. So, we provide a fresh approach to solve this issue. To defend against shoulder surfing attacks, we have created two ideas. To start, the user must create one if there is no registration. Second, you need to sign in using a legitimate user ID and password. It is the password an assortment of letters and digits. Third, the user must pass an image-based authentication process where they can select the likelihood of a password and this strategy working against one other is greater. You should select a password based on your registration. password must match when logging in. You need to upload an image of your choice, then the image is divided into four parts. Multiple images should be selected in graphical password authentication, and You must remember the password sequence. Like three-factor authentication, too. So, this is proposed a new graphical password secure authentication system that is resistant to shoulder surfing as well as other forms of attacks and probable assaults.

Article History
Article Received: *15 October 2022*
Revised: *24 November 2022*
Accepted: *18 December 2022*

Key Words: Computer Authentication, Graphical Password, Computer security.

I. INTRODUCTION

Graphical password secure authentication system is the name for an authentication method that relies on more than one factor when determining whether to grant access to a computer user.[1] It has become an increasingly important means of proving identity and securing information. From the moment the first treasure was amassed, limiting access to it became a priority. If buried in the ground, knowledge of the location was critical. A key was required if a locked chest or storage room were involved. If guards were posted, recognition of the rightful owner was vital. Today data is a great treasure that must be secured, but protecting it still often involves these elemental factors: knowledge, possession, and inherence. In other words, access is granted or denied depending on what someone knows, what someone has, or what someone uniquely is.

II. OBJECTIVE

The goal Graphical password secure authentication system of is to create a layered defense that makes it more difficult for an unauthorized person to access a target, such as a physical location, computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one or more barriers to breach before successfully breaking into the target. Protection of access to identity data with strong authentication mechanisms.[2] Provides adaption and improvement of cryptographic methods to securely store and share identity data in the cloud.

III. LITERATURE REVIEW

We adapted the study methodology for the literature review of Multi-Factor Authentication
The protocol to better fit our research needs. Methods utilized in our research involve the following steps:

(1) Data Collection through database search,

(2) Data Screening involving: Title screening

During our systematic literature review, we investigated the existing set of literature based on user studies in multifactor authentication for paving the path for future studies by underlining existing gaps in research Risk perception analysis is extremely helpful in understanding the risk of security challenges. We identified the majority of research on risk perception is focused on usability and password memorability.[6] Table 1 shows the different types of risk analysis the studies performed; tool risk trade-off understanding was studied for 5% of the paper which was an interesting finding since many research claims that there is a misalignment of user risk perception with tool's utility. Nudging was considered as a primary method to interject into the risk mental models of the users. While MFA is gradually gaining popularity, password authentication still dominates the area of single-factor authentication and the first factor in MFA authentication. We saw that 16% of the user studies focused on understanding the password security understanding of the users. We found that security researchers are particularly interested in password creation and management.

IV. METHODOLOGY

In this paper when any user tries to access the Homepage, they will be provided with three options register, login, and about developer.[5] If you have not registered yet, then you must click the register option.

1) Then the register page will appear, you must provide first text base password and necessary information like first name, last name, email, password, security question etc.

2) After clicking next Image base password page will appear, you have to select multiple images as a password and save it.

3) After clicking to proceed next Google authentication page will appear, you have to register by scanning the barcode from your mobile.

4) Then you have to come back to the home page, then you have to click on login. After that, you have to provide the username and correct password. If text base username and password are correct, then you have successfully login in textbase password.

5) Then the Image base password page will appear, after that, you have to select the image base on

the password. If it is correct, you have successfully logged in to the image base password. 6). Then you have to authenticate by using Google authenticator. You will be redirected to the main page

V. FLOW CHART

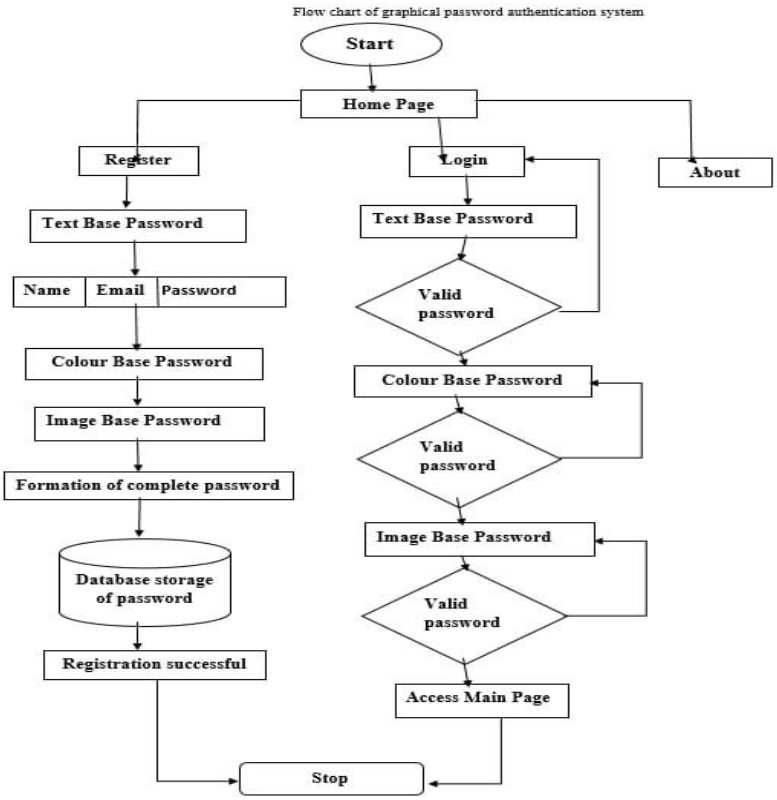

Fig 1: Flow chart of system authentication

I. ANALYSIS AND RESULT

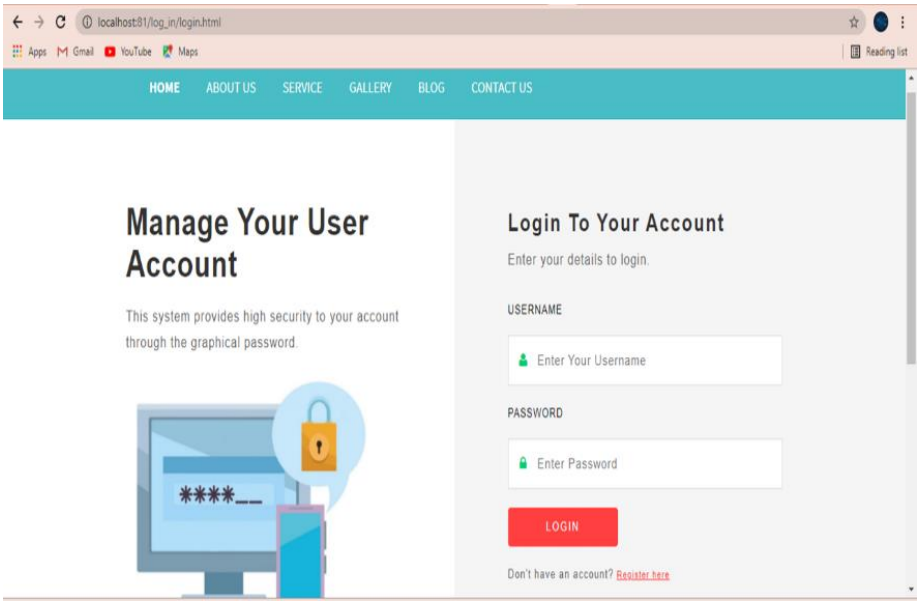

Fig 2: Registration page

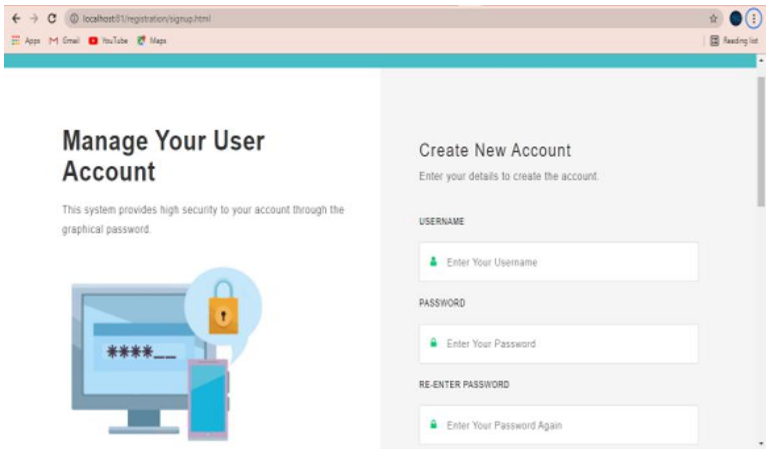

Fig 3: Sign up

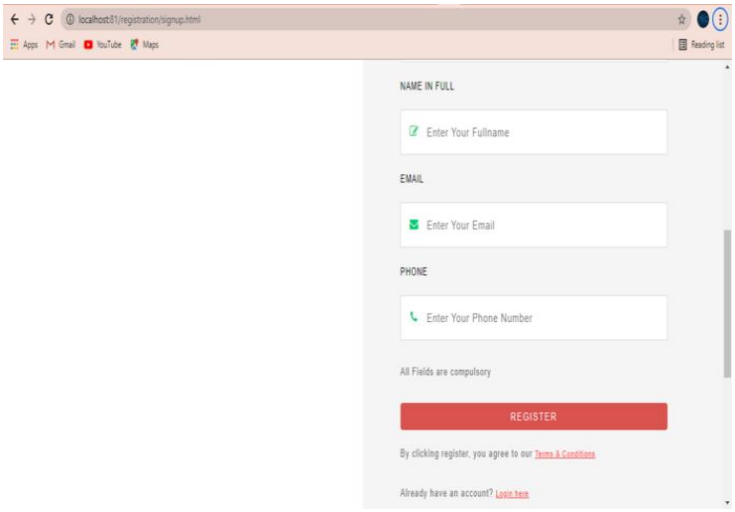

Fig 4: Personal Details

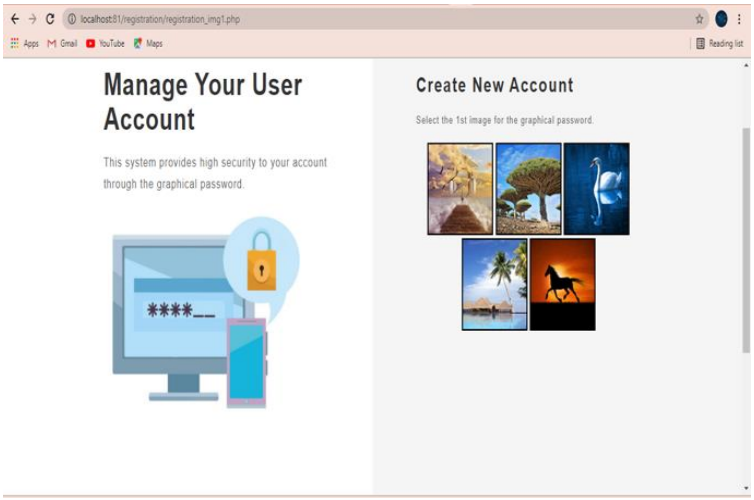

Fig 5: User Page

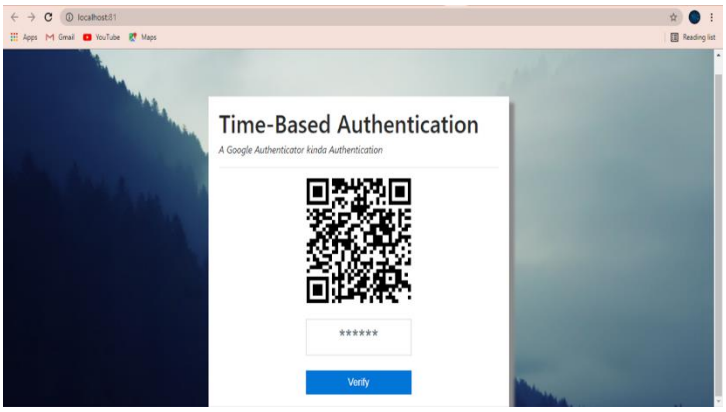

Fig 6: Time-Based Authentication

The screenshots of the results of the designed system are shown in the above figure.

1) Then the register page will appear, you must provide the first text base password and necessary information like first name, last name, email, password, security question, etc.

2) After clicking the next Image base password page will appear, you have to select multiple images as a password and save it.

3) After clicking to proceed next Google authentication page will appear, you have to register by scanning the barcode from your mobile.

4) Then you have to come back to the home page, then you have to click on login. After that, you have to provide the username and correct password. If text base username and password are correct, then you have successfully login in textbase password.

5) Then the Image base password page will appear, after that, you have to select the image base on the password. If it is correct, you have successfully logged in to the image base password.

6). Then you have to authenticate by using Google authenticator.

7) Then the main page will come.

Below is a table which explains various features of the project.

II. CONCLUSION AND FUTURE ENHANCEMENT

Digital devices are becoming part of our life day by day. By using digital devices, we have able to know about the authentication process. Validation is an integral part of security. Authentication will give the customer greater security. Specific review articles research in the same field about the specific assaults found during validation. Printed hidden-term authentication is an excellent testing device. It is more useful and secure compared to previous old base graphical password authentication systems. Since the password space is very large, it offers security against brute-force attacks. It's easy to use. Passwords can be easily created and recalled. The randomization in both authentication system provides strong security against

Comparison	Text-Based	Color Based	Image Based
Security	Less	Highest	Highest

Required Cost	Nothing	Less	Less
Usability	Easy	Easy	Easiest
Availability	Always	Always	Always
GUI	User Friendly /Not attractive	User-friendly / Attractive	User-Friendly / more Attractive

Table 1: Comparison Between Technologies

shoulder surfing. To have a good system, you need high security and good usability, and can't be separated them. Shoulder navigation attack is subject to safety precautions.

However, the proposed methods for the shoulder surfing problem still need to be improved. This system can also be used to add a higher level of security to the text-based password system. This system is very cheap compared to a biometrics system.

REFERENCES

[1] Graphical Password Authentication. Shraddha M. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.

[2] Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015

[3] The Shoulder Surfing Resistant Graphical Password Authentication Technique. Mrs.Aakansha S. Gokhalea , Prof. Vijaya S.Waghmareb.

[4] A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K.

[5] Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme. Prof. S. K. Sonkar, Prof. R. L. Paikrao , Prof. Awadesh Kumar, Mr. S. B. Deshmukh, Computer Engineering Dept. Computer Engineering Dept. Amrutvahini College of engineering, February - 2014

[6] A Graphical Password Against Spyware and Shoulder-surfing Attacks. Elham Darbanian Master of Engineering, College of e-learning Shiraz University, Gh. Dastghaiby fard Department of Computer science & Engineering, College of Electrical and Computer & Engineering Shiraz University,jun- 2015.

[7] Text based Graphical Password System to Obscure Shoulder Surfing. Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir Department of Computer Science COMSATS Institute of InformationTechnology Islamabad Pakistan, 13th January,2018

[8] Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar,"Tensorflow-Based Automatic Personality Recognition Used in Asynchronous Video Interviews", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[9] Mohammed Shoeb, Mohammed Akram Ali, Mohammed Shadeel, Dr. Mohammed Abdul Bari, "Self-Driving Car: Using Opencv2 and Machine Learning", The International journal of analytical and experimental modal analysis (IJAEMA), ISSN NO: 0886-9367, Volume XIV, Issue V, May/2022

[10] Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics AtEducational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6,Issue 12, December 2021,Page 43-46

[11] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021

[12] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering(Toronto) Elsevier SCI Oct

[13] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

[14] Dr. M.A.Bari, "EffectiveIDS To Mitigate The Packet Dropping Nodes From Manet ", JACE, Vol-6,Issue -6,June 2019

[15] M.A.Bari & Shahanawaj Ahamad," Process of Reverse Engineering of EnterpriseInformation System Architecture" in International Journal of Computer Science Issues (IJCSI), Vol 8, Issue 5, ISSN: 1694-0814, pp:359-365,Mahebourg ,Republic of Mauritius , September 2011

[16] M.A.Bari & Shahanawaj Ahamad, "Code Cloning: The Analysis, Detection and Removal", in International Journal of Computer Applications(IJCA),ISSN:0975-887,ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38, NewYork,U.S.A.,April 2011

[17] A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices. Teoh joo Fong, Azween Abdullah , NZ Jhanjhi School of Computing & IT, Taylor?s University, Subang Jaya, Selangor, Malaysia, 2019

[18] Security in Graphical Authentication. Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee Department of Computer Science and Engineering, Qatar University, Doha, Qatar, May, 2013.

[19] Kathole, A. B., Katti, J., Dhabliya, D., Deshpande, V., Rajawat, A. S., Goyal, S. B., . . . Suciu, G. (2022). Energy-aware UAV based on blockchain model using IoE application in 6G network-driven cybertwin. Energies, 15(21) doi:10.3390/en15218304

[20] Keerthi, R. S., Dhabliya, D., Elangovan, P., Borodin, K., Parmar, J., & Patel, S. K. (2021). Tunable high-gain and multiband microstrip antenna based on liquid/copper split-ring resonator superstrates for C/X band communication. Physica B: Condensed Matter, 618