iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41621

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 10 Issue IV Apr 2022- Available at www.ijraset.com

Graphical Password Authentication System

Pathik Nandi[1], Dr. Preeti Savant[2]
[1]*Master of Computer Application, Dept. of Information Security Management System, Jain (Deem-To-Be University), Bangalore*
[2]*Assistant Professor, Dept. of School of CS & IT Jain (Deem-To-Be University), Bangalore*

Abstract: ***Graphical password is one of technic for authentication of computer security. Now days digital/computer security is most important things in computer science for protected user or customer data. And Shoulder-surfing is a one of the threats where a criminal can steal a password by direct observation or by recording the authentication session. There are several techniques available for this authentication, the most prevalent and simple of which is the Graphical password technique. So, we suggest a new technique to combat this problem. We have developed two concepts to combat shoulder surfing attacks. First, the user must register if the registration does not exist. Second, you must log in with a valid user ID and password. The password is a grouping of characters and numbers. Third, user has to cross image-based authentication where user can choose their password and this method have higher chances to offset each other. You should choose password according to the registration password, it must to match at login time. In colour base authentication, there should be several colour base passwords and depending on the colour, you need to remember the password sequence. And it's like three-factor authentication. So, here is proposed a new graphical password authentication technique that is resilient to shoulder surfing and also to other types of probable attacks.***

Keyword: Computer Authentication, Graphical Password, Computer security

I. INTRODUCTION

Graphical password is one of process for authentication in computer system. computer security is create a safe zone for our digital devices. Graphical password is a one of the processes to provide our security of digital device or important information. As we know that our human brain can easily store or recall an image or image-based password. So, we propose graphical password for user who can register random with highly secure and there is no difficulty to recall the graphical password. Authentication is a data access point that manages consumer security assurance. It is a process that grants in a particular context requiring the customer to. Validation schemes are categorized as token-based authentication, validation based on biometrics, validation based upon knowledge. Tokens are used as a Hidden Key in token-based authentication.

As the name suggests, it uses different types of shapes and images as password. In addition, scientist is saying that it's easy to remembered a picture for human brain than text. The human brain can easily process images. And image base password, it is resistant of dictionary attack, keylogger, social engineering etc.

Alphanumeric password is an old traditional common authentication method. Practically this traditional method is too unsecure system. For example, attacker may choose easily guessed user's password, if user is not using a strong password. User may use same password for multiple device or site. This are all unsecure characteristic for normal users. And authentication is one of the important security points where user has active responsibility for their personal information security.

Generally graphical password techniques are two types: [1] recognition-base and recall based graphical techniques, [2] recall based graphical techniques.

In recognition-based techniques. User has to authenticated by choosing one pr more images which he chooses during the registration time. In recall-based techniques is a process that user has to remember that was done during registration time.

II. LITERATURE REVIEW

"Graphical Password Authentication" by Shraddha M, Leena S. Gawade, Prathamey K. Rane. [1] They designed a graphical password technique wherever they have presented some of impotent technic of graphical password for example multiple-image base password that some number of pictures can offer to user and that they need to select one or more of them. Next grid base scheme, which is easy object there aren't any further displays are required. Next Triangle scheme, which is provide with protrusive surface and numbers of images shown are virtually same, it's tough to choose out. Most impotent things in this paper is that calculate base of username. So, this is often new scheme provides solves the numerous issues of existing system.

"Enhancement of Password Authentication System Using Graphical Images" by Amol

©IJRASET: All Rights are Reserved

Bhand, vaibhav desale, Swati Shirke, Suvarna Pansambal.[2] In this paper mainly focuses on the construct of graphical password system completely with different authentication systems. And also, the basic goal of this method is to attain higher security with easy technique to use by a user and more durable to guess by hacker. So, they develop 3 different kind of authentication system A. Pass point, B. Cued Click Point, C. Persuasive Cued Click Points. Pass point, during this system user should choose 5 points from single picture and at the time of choosing and through the time of login user has to repeat identical sequence of the points from single image. And Cued click point has the same construct as of the pass point however the most distinction between them is passing 5 points on five completely different image one point per image. PCCP could be a authentication technic. PCCP is a best technology but it has security issues connected with it.

"A New Graphical Password Scheme Resistant to Shoulder-Surfing" by Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin.[4] In this paper they are discuss about security features of graphical authentication. Different graphical password schemes have different techniques to scale back the cyber-attacks. As you recognize that graphical password is simple to remember and high usability with high security. So graphical password schemes are provided higher security than text -based passwords. Some of the resistance of graphical password authentication attacks are shoulder surfing, brute force, dictionary attacks, guessing attack, spyware and social engineering attacks. During this paper they supply a quick description and classification of various graphical password schemes followed by information about vulnerabilities within various schemes and suggestions for future development.

III. PROBLEM STSTEMENT

Alphanumeric password is an old traditional common authentication method. Practically this traditional method is too unsecure system. For example, attacker may choose easily guessed user's password, if user is not using a strong password. User may use same password for multiple device or site. This are all unsecure characteristic for normal users. And authentication is one of the important security points where user has active responsibility for their personal information security. If we use old traditional password system then there may have possibility to dictionary attack, Brute Force Attack.

IV. COMPUTER AUTHENTICATION:

Authentication is a process where user show their identity to their system or server. A common example is entering a username and password when you login to a website. There are several authentication types.

1) Single-factor authentication (SFA).
2) Two-factor authentication (2FA).
3) Multifactor authentication (MFA).

Authentication allows real users to access the computer. And if the authentication does not match, then it will be denied to the unauthorized person. Authentication technique used by any digital system or site where the system or site needs to know the actual authorized user. Even authentication used to determine which resources the user accesses and which resources are denied access, at time the user can access the resource and how much of the source the user can consume. Typically, Authentication by a server generally involves the use of a username and password. Other forms of authentication can be included cards, retina scans, voice recognition, and fingerprints. Authentication by a client generally involves the server providing the client with a certificate that a trusted third party, such as a bank, expects from the clint to do. Authentication does not determine what activities the person can perform or what file the person can see. Authentication simply identifies and verifies who the user or system is.

The main purpose of authentication is to allow authorized users access to the computer and to reject access to unauthorized users. Operating systems typically identify/authenticate users using three ways: Passwords, physical identification, and biometrics. These are explained below.

A. Passwords

Password is a secret text which is combination of characters, numbers and symbols that used to verify the user's identity during the authentication. Password is very important secret key for digital devices or site. User need to create username & password for secure our important information. Server has stored all username & passwords. When any user tries to access any information, user has to verify their username and password by comparing with login system.

If username and password are match then system will allow to access all information.

B. Physical Identification

Physical identification used in organizations such as education department, company or any office. Now that the technology is too advanced, an organization are set a authentication machine that will give allow all authorize person in organization. For example, an employee has an employee id card to identify in their organization, so before taking up his duties he must authenticate himself with his ID card, which is called physical identification and this system will protect against people who are not authorized who cannot enter the organization without authorization. For any organization, they have to worry about physical security which will help to protect from any threat. In our daily life, we use ATM smart cards, which are best example of physical identification. Therefore, the ATM system is a combination of password and card identification. This allows the authentication without storing password or card information in the computer system.

C. Biometrics

In biometrics, bio means 'human' and metric means 'measurement'. In simpler terms, biometrics is any measurement related to human characteristics that makes an individual different from other individuals. Biometric authentication refers to a unique security technique that involves our biological characteristics such as voice, fingerprints, eye retinas etc.

V. GRAPHICAL PASSWORD

As the name suggests, different types of images or shapes are used as a password. In addition, a scientist says that human brain can easily store images than text.

The human brain can easily process images. so, engineers offered a graphical password authentication system which is very simple to use and very simple to recall their password. And graphical password is more secure than text-based password which is resistance of dictionary attack, keylogger, social engineering etc. In general, graphical password techniques are two types: recognition-based and recall based graphic password.

In graphical password we used 2 types of authentications first is colour-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 very unique for authentication system. 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.

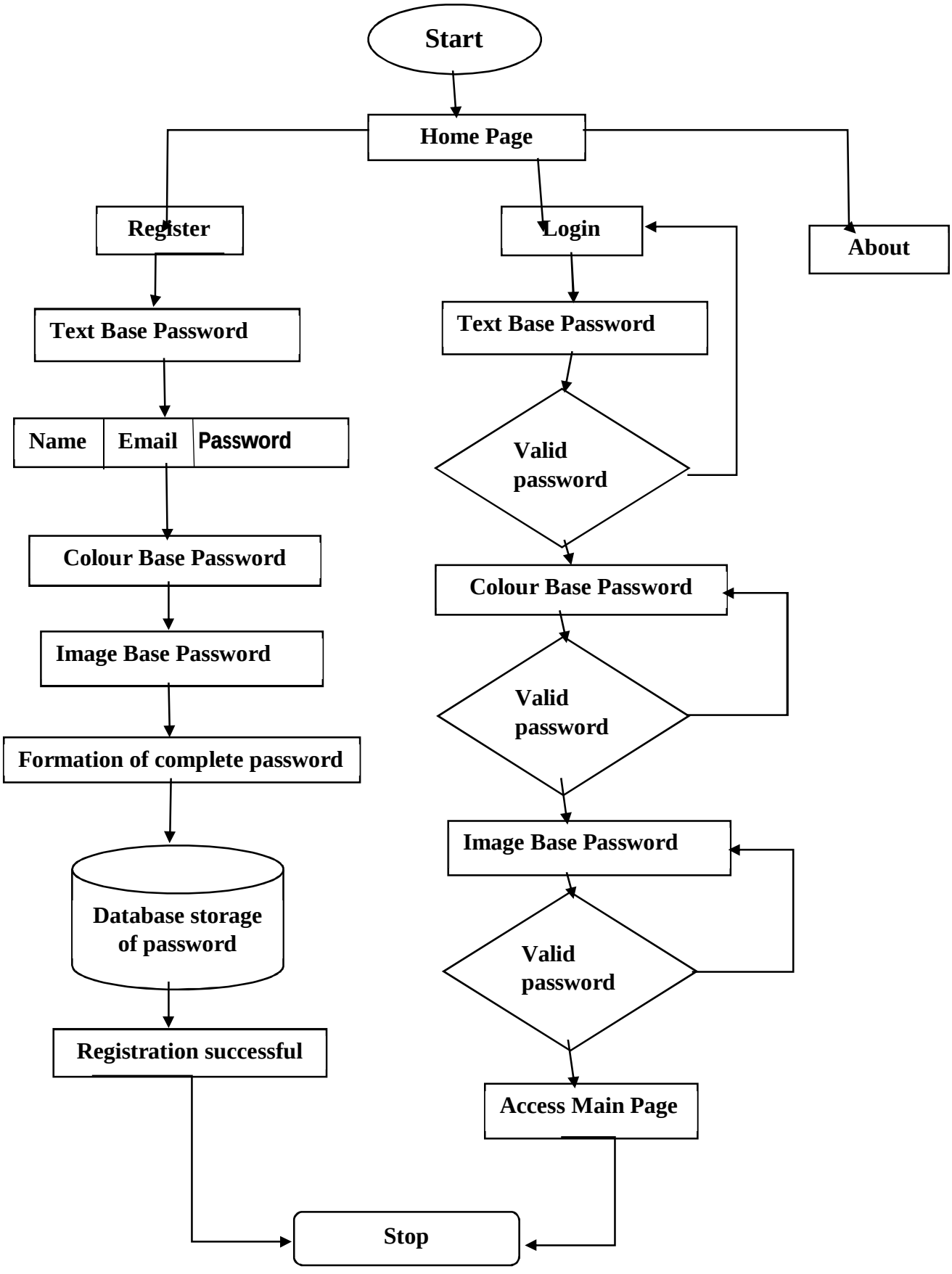
VI. METHOLOGY

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

1) Then register page will appear, you have to provide first text base password and necessary information like first name, last name, email, password, security question etc.
2) After clicking next Second colour base graphical password security page will appear, then u have to select password squatly. And you have to remember squatly base on colour.
3) After clicking next Image base password page will appear, you have to select multiple images as a password and save it.
4) Then you have to come back to 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 text base password.
5) Then colour base password page will appear, after that you have to give colour base password. If it is correct, then you have successfully login in colour base password.
6) Then Image base password page will appear, after that you have to select image base on password. If it is correct, then you have successfully login in image base password.
7) Then main page will come.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Flow chart of graphical password authentication system



©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

VII. RELATED WORK

Graphical passwords refer to using images and different colour 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 is more attractive and visual representations that are used in place of text or alphanumeric characters.
The graphical passwords consist of six sections namely:

A. Image Based Scheme

In this scheme, the number of images will be provided and the user will need to select images as the password. From the grid, the user must select the actual images in a correct order for authentication. User can easily remember the password as show in the pictures. Image base password are more attractive and images are repositioned for every login attempt. So, this scheme come close to avoiding from shoulder surfing attack. These classes define appropriate weak password subspaces for an attack dictionary.



B. Colour Base Scheme

In this scheme, the number of colours will be provided and the user will need to select colours as the password. In this system, different colours are used to confuse the imposters, but easy to use for authorized users. User can easily remember the password as show in the colours. It is resistant to shoulder surfing attack. User has to select the real colours in a correct sequence for authentication. Then password will save in database.



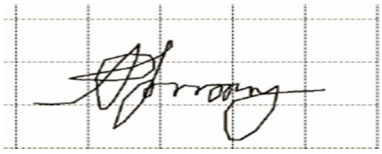


C. Recognition Based

With this technique users set an image as a password during registration. User must reproduce or remember their own passwords, and thus no hints are given to remember the passwords. The user must select the specific number of images in this set as a password. During authentication, the user must correctly recognize these preselected images.[2]

D. Signature Based Scheme

In this scheme, the user's signature is used for the password mentioned in the system. Anyone's signature cannot be copied as it is. A small error in the signature can prohibit the access.

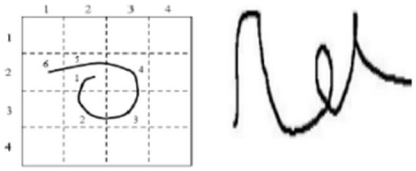


©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

E. Pure Recall Based

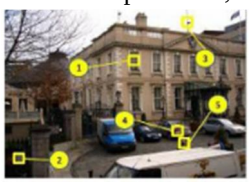
Pure recall authentication system is difficult for users to remember. Some pure recall authentication system published result offer higher level of entropy than text-based password. This scheme requires users to draw the password on a grid or a blank canvas. The user must redraw such that the drawing to touch the listed sequence of coordinates. It is more secure than the recognition-based technique but it is very difficult for users to remember their passwords.



F. Cued Recall Based

In this scheme, during the registration phase, the user must select multiple clicks points on an image in a specific order. Then the user must select the same click points in the same order while the user selected the same order of the click points selected in the registration phase.

These techniques provide hints to the user to remember the password, so they are simpler than pure recall-based techniques.



VIII. ANALYSIS AND RESULT

A. User Friendly of Graphical Password

Graphical password is a user-friendly authentication system. User friendly authentication means we can use this system everywhere like any device or any site. It is very easy to use and everyone can easily remember their password. This graphical password system is an alternative solution for text-based password. Graphical authentication system, where a user can register randomly and it's more secure password than others. In this system main characteristic, there is no difficulty in remembering the registered password. The basic goal of this system is to achieve higher security with easy technique to use by a user and difficult to guess by a hacker.

B. Application

We are using digital devices everyday where we have to come cross an authentication process every time. graphical password is a user-friendly authentication system. So, we are approaching to use everywhere like on web development, desktop level and any other application level. Some applications which are presently using graphical password authentication systems.

- Web application.
- Mobile system.
- File locks system.
- Desktop security level.

C. Security Analysis

Graphical password system offers a strong security against brute force and guessing attacks as it has two level of graphical passwords system. The password system is difficult to guess the password system by a person and it is a shoulder-surfing resistance system. It has a very large password range. For this project we used 3 level of security authentication following

For step1: Authentication of text base password.

For step2: Colour Base Authentication.

For step3: Image Base Authentication

1) *Brute Force Attack:* Brute force is a digital attack where the attacker tries to guess the correct password. So, to defend against brute force attacks they system should have a large combination of password which is very difficult to remember for human. Instants of large text password we create a graphical password interface. It is very difficult to guess the correct password.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2) *Spyware:* Spyware is another possible attack mechanism for graphical passwords. There are several types of spyware including keyloggers, hijackers and spybots. Spyware collects information entered by the user. With graphical passwords, it is more difficult to conduct spyware-based attacks because it is harder to copy mouse motions exactly. Combinations of pass images and CAPTCHA may be especially resistant to spyware
3) *Shoulder Surfing:* Shoulder surfing refers to looking over someone's shoulder in order to obtain information such as password, PIN and other sensitive information. This type of attack is more common in crowded areas where it is not uncommon for people to stand behind another queuing at ATMs.

Comparison Of Password Technologies

Comparison	Text Based	Colour 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

IX. CONCLUTION

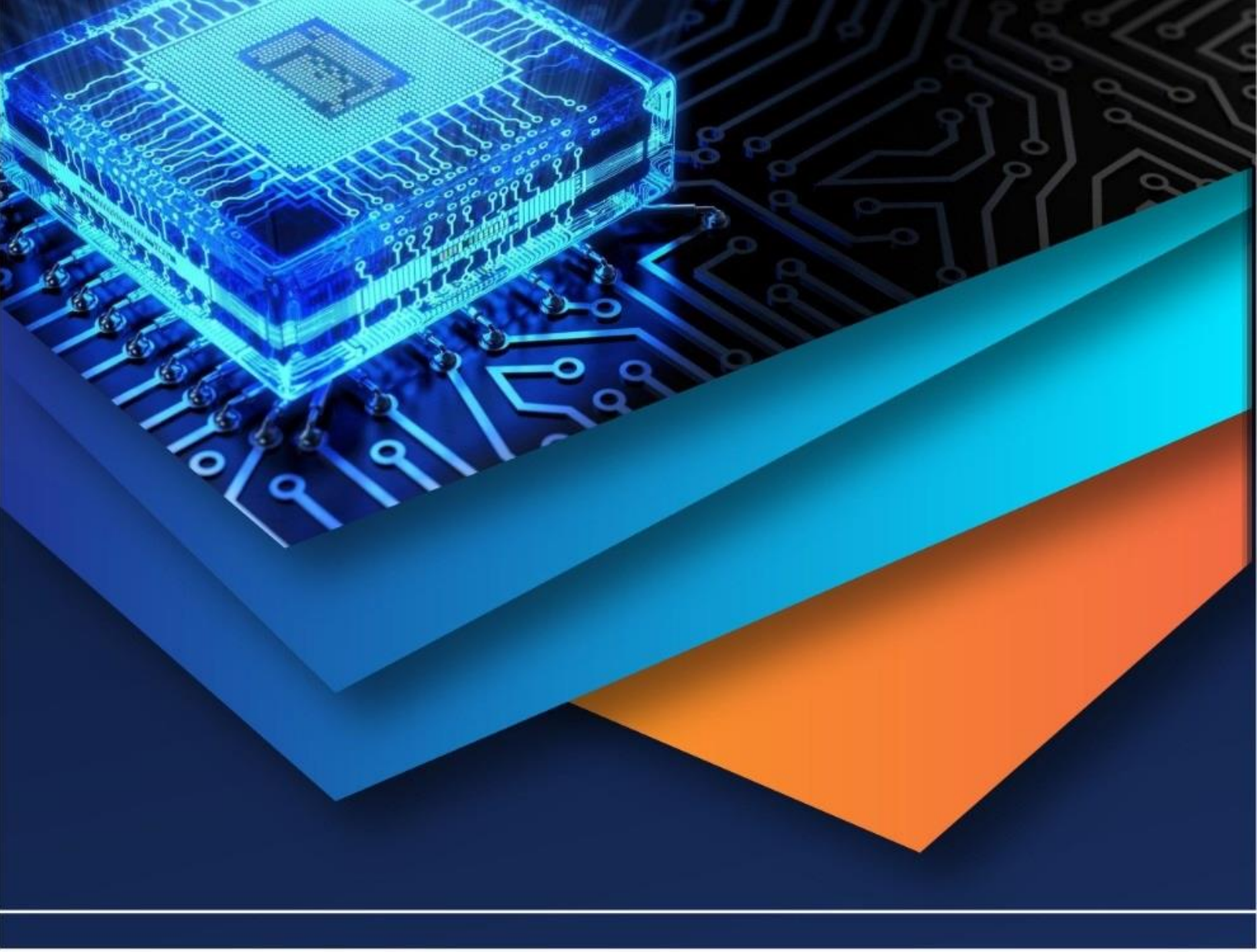
Digital devices are becoming part of our life day by day. By using digital devices, we have abled to know about authentication process. Validation is an integral part of security. Authentication will give the customer greater security. Specific review articles research in the same field about the specific 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 recall. The randomization in both the authentication system provides strong security against 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 precaution. However, 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 as compared to a biometrics system.

REFERENCES

[1] Graphical Password Authentication. ShraddhaM. 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] 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
[9] 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.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)