International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2494-9150 Special Issue-01, MAR 2016.

COLOR SCHEME AUTHETICATON

[1]Prof. Vishal Shinde, [2]Gunjan Patil, [3]Namita Ghanghav, [4]Sambhaji shinde
[1]Asst. Professor, [2,3]BE Student, [1,2,3]Comp. Engg. Dept, SSJCET, Asangaon, India.
[1]mailme.vishalshinde@redfimail.com, [2]patilgunjan94@.com, [3]ghanghavnamita93@gmail.com,
[4]sam.bhaji.shinde80@gmail.com

Abstract: There are no of methods used for the authentication purpose; in which the textual password is most common. But these textual passwords are susceptible to various kinds of attacks such as, Shoulder Surfing, Eavesdropping etc. Due to these reasons the graphical password scheme has been introduced. The authentication of the user in this scheme is done by using the session password. Session passwords can be defined as the password that can be used only once. But on the other hand these graphical passwords have their own disadvantages such as time required to authenticate the user is more. This session passwords once they are terminated, these passwords end up with their life-Span. But at the same time these session passwords is very much useful in the security purpose as they provides better sorts of security against the Brute force attack, Shoulder Surfing attack and Dictionary Attack. The proposed authentication scheme consists of the texts and colors for generation of session password the textual password are the one that have used commonly. But these textual passwords have their own risk of security against the attacks.

Keywords-*color based codes, pair based authentication scheme, textual passwords scheme, session passwords, Attacks.*

I. INTRODUCTION

Authentication is any sets of rule that allows one entity to recognize the identity of another entity. This authentication must be first secured in order to protect the user account. Traditionally the textual passwords are commonly used as they are convenient and also familiar to most of the users, it can be used easily and their implementation is also cheap. As it is mentioned that the earlier passwords are used to secure a system but when the password is lengthy it becomes very critical job to remember those passwords which would secure the system. Thus the user picks the short passwords which could be remembered easily but again it has its own dis advantages that it can be cracked easily by the hacker. Thus the graphical passwords can overcome these kinds of attacks but this technique also has limitations as time required is more for authentication and it is quite expensive.

Thus in proposed system there is a generation of a new authentication scheme in which the concept of session password is use. Session passwords are nothing but one time passwords once they are used they end up with their life span. Therefore the combination of text as well as colors is used where some colors pairswould be allocated to some of the text during login. Their graphical passwords authentication scheme has not been adopted widely.

II. LITERATURE SURVEY

Various comprehensive investigations on the existing authentication schemes have been accomplished. And it has been discerned that none of the recent authentication schemes can resist all sorts of attacks.

With this outcome, this report propose authentication scheme which overcome all the existing authentication schemes.

a) DHAMIJA AND PERRIG

The given graphical scheme of authentication which proves that the user is authorized just by identifying an appropriated pre-defines images. In this given scheme, the user has to select the images from the set of pre-define images which has given from the registration process. And after the process of the registration the user has to select the same images that have been selected during the registration for login. So as to prove the user identity is authorized, but shoulder surfing token based is a kind off attack where this system is vulnerable, but if the biometric is taken in to an consideration for the authentication both text based and the pair based techniques included. Therefore Dhamija and perrig proposed a scheme of graphical authentication which is based on hash visualization techniques. Due to the use of these techniques the various attacks are lowered.

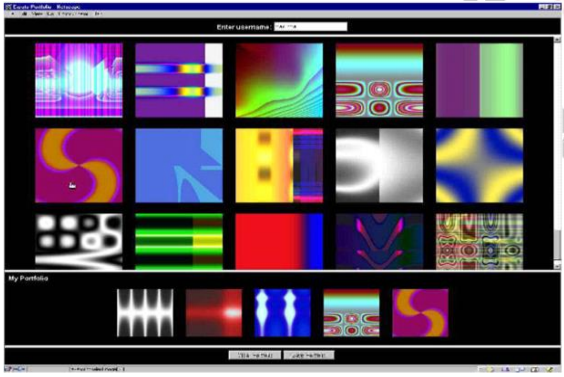


Fig a: - Image Authentication

b) PASS FACE

Due to the dis-advantage that occurred earlier. A new type authentication is introduced which is known as pass face as the name suggest pass face we consider grid of a faces and from that a faces the user has to select an image. And from that grid 4 images should be selected by the user as the password in order to start the process of pass faces.

Real user cooperation had develop the process of pass faces. The idea behind this process is as follows and from selected images which get the password for his future use. The next step is a authentication step in which grid of image will be displayed which will see by the user instant of further decoded images. The previously chosen images will also be displayed. The user will select the image as per the choose

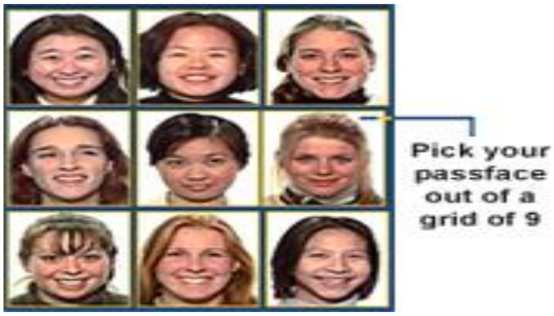


Fig b: -Pass faces Recognition

c) JANSEN

Jansen proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the correct sequence. One Drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size. Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication. The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification.

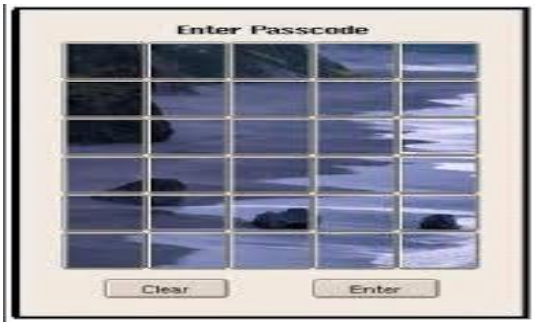


Fig c:- Pass code process

d) STORY SCHEME

To overcome this shoulder surfing attacks a scheme was proposed by Haichang.This schemes is combination of DAS and story schemes. The user has to draw a curve along the images to prove their authenticity. Jansen proposed a graphical password scheme for mobile devices. Consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence will create a numerical password.

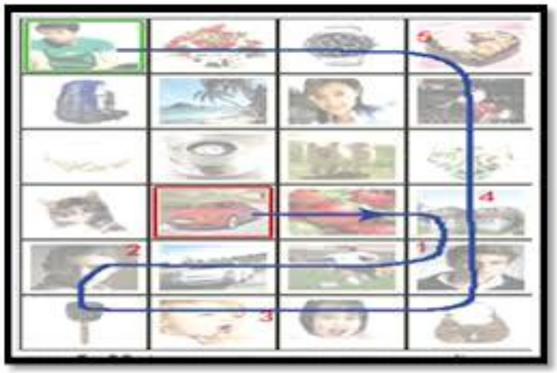


Fig d:-Story Scheme Recognition

Thus story scheme is used to but on the other hand it has its own dis advantages. Hence in order to avoid that another new technique was taken in to consideration.

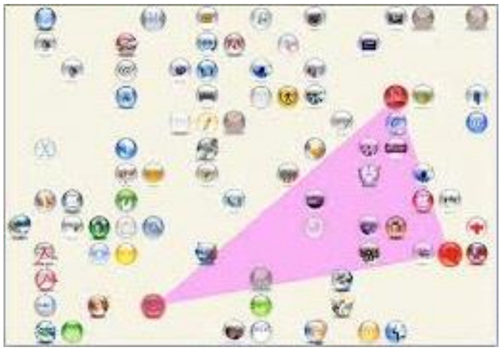
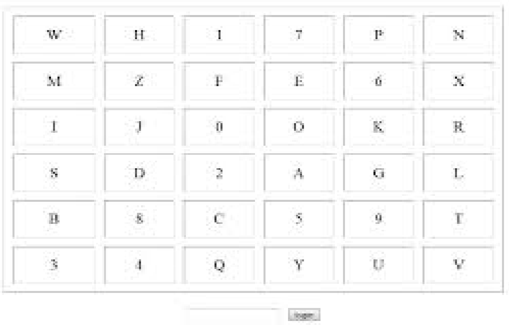


Fig d.I:-weinshall

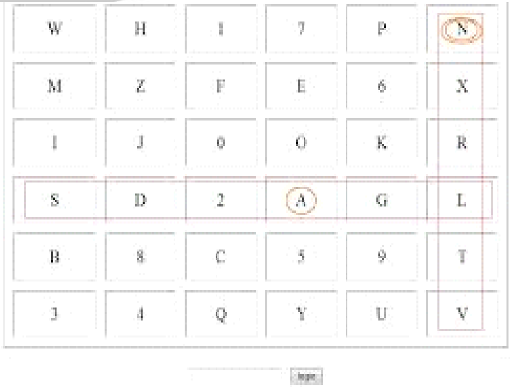
e) PAIR BASED AUTHENTICATION

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. These are randomly placed on the grid and the interface changes every time.Information and computer security is supported largely by passwords which are the principle part of the authentication process.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig e: - Pair based scheme



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig e.I:-Pair base selection

- SECURITY ANALYSIS

The occurrence of the session password changes due to the change in the interface. Hence shoulder surfing would be resisted due to this technique. Therefore dictionary attack can be avoided due to dynamic password.

- DICTIONARY ATTACK

Textual passwords are one on which there is a risk of dictionary attack. Dictionary attack is a type of attack in which the hacker first makes the set of words of dictionary and tries those words one after another in order to authenticate..

- SHOULDER SURFING

Information and computer security is supported largely by passwords which are the principle part of the authentication process. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information

- BRUTE FORCE ATTACK

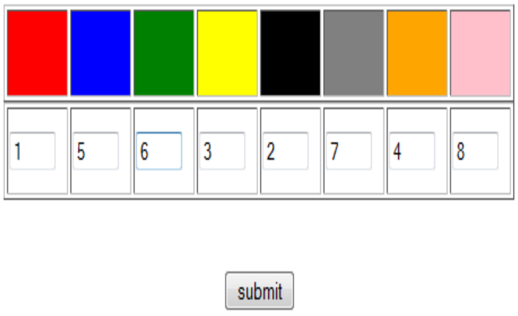
These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility. It is atrial and error method used to obtain information such as user passwords or personal identification number. In a these attack automated software is used to generate a large number of consecutive guesses as to the value of the desired data.This attack may be used to crack the encrypted data. Brute force attack may also be referred as brute force cracking.

III EXISTING SYSTEM

Sr No	Authentication schemes	Attack	Usability	Security	Password space	Implementation
1	**D**hamija &**p**errig	shoulder-surfing	High	Very low	More	Easy
2	Pass faces	Thwart guessing attacks	High	Low	Quite less	Complicated
3	Jansen	Dictionary Attack	Less	Low	Quite less	Complicated
4	Story scheme	Eavesdropping,	Very high	Very high	Less	Less Complicated
5	Pair-based authentication scheme	man-in-middle attack	Very high	High	Less	Easy

IV PROPOSED SYSTEM

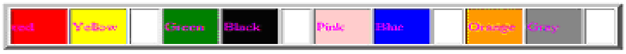
A new authentication scheme named "Color Scheme Authentication". In these proposed system authentication is done on both colors and numbers instead of words. Due to the use of matrix the user have to select the values from 1-8 for the given 8 colors. These authentication processes are risk free of shoulder surfing, eves dropping, Dictionary attack etc. the process of authentication is evolved as each and every user can select or can give the colors as per their choice.

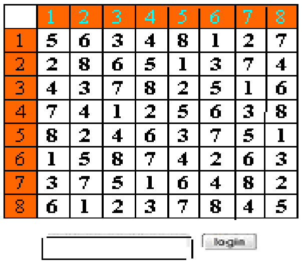


1	5	6	3	2	7	4	8

FigIV: - color rating

"RLYOBGIP" different colors occur.





	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig VI.1:- Color code matrix

Therefore after the registration process next step is of login phase. In these login phase user has to enter the user id so as an interface is generated which is based on the colors the user select. In these login phase there is a grid of 8*8 matrixes the numbers from 1-8 is displayed in any random sequence the strips of colors is also contained by an interface. These color grids consist of 4 pairs of colors which represents these grids as rows and columns. Due to the rating which is given to the colors a user receives a session password.

a) SYSTEM ARCHITECTURE

For authentication the user 1st enters his unique user ID. Then click on the "NEW" button .At the same time a onetime key of random no is issued by the system and then it is send to the user's mobile number given at the registration stage. For example let consider the key which is obtained by user is386. Now the system displays four colors that have assigned to each of the single character.

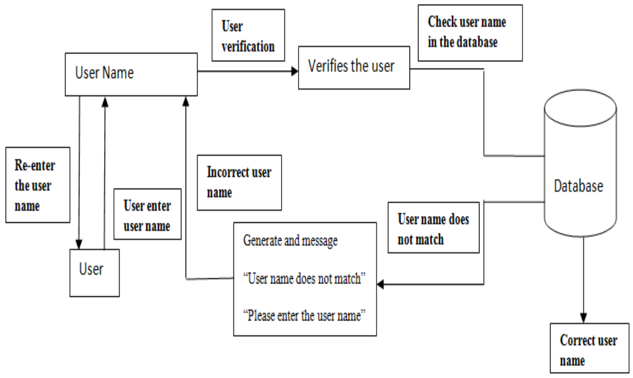


Fig a: - Login process

V MATHEMATICAL MODEL

The system mathematically represented as follows:

$M = \{\Sigma, \delta, O, T\}$

$Where \Sigma = \{C1, C2, C3, C4, C5, C6, C7, C8\}$

$(CRi) i = 1\ to\ 8 = \delta\{Cj \mid 1 \le j \le 8\ and\ 1 \le i \le 8\}$

$T = \{CP, G\};$

Where

$G = \{x(I, i)\};$

$CP = \{CP1, CP2, CP3, CP4\}$

Where

$CPi = x, y;$

Where x, y can be colors from $C1, C2, C3, C4, C5, C6, C7, C8$

$G = \{rand\ (i, j) \mid 0 < i < 9\ and\ 0 < j < 9\}$

; *where*

$P2 = \{G\ (i, j) \mid where\ i = CR\ (CPi1), j = CR\ (CPi2)\};$

a) ALGORITHMS

Rijndael (pronounced rain-Dahl) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists that were themselves selected from an original list of more than 15 submissions. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys9 rounds if the key/block size is 128 bits

11 rounds if the key/block size is 192 bits

13 rounds if the key/block size is 256 bits

Rijndael is substitution linear transformation cipher, not requiring a fesital network.

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule

2. Initial Round

1) AddRoundKey—each byte of the state is combined with the round key using bitwise xor

3. Rounds

1) Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2) Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

3) Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

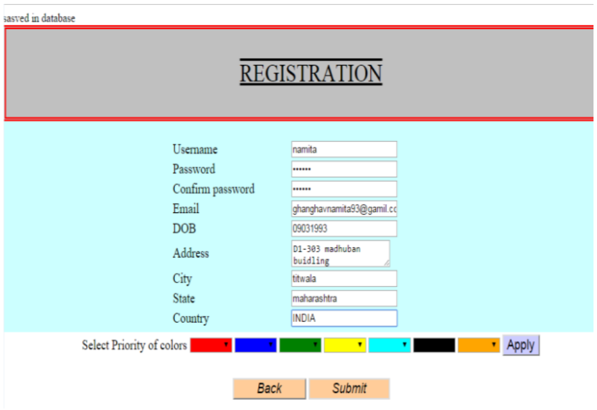
4) AddRoundKey

4. Final Round (no Mix Columns)

1) Sub Bytes
2) Shift Rows
3) AddRoundKeys

VI EXPECTED OUTPUT

The input design is very important for any application. The input design describes how the software communicates within itself, to that interested with it and with human who use it. The input design is the process of converting the user-oriented inputs into the computer-based format. The data is fade info the system using simple interactive form. The form has been supplied with message so that user can enter the data without facing any difficulty. The data is a validated where ever it is required.



sasved in database

REGISTRATION

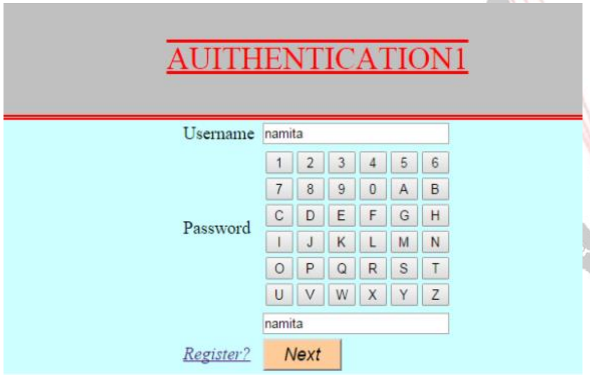
Username	namita
Password	••••••
Confirm password	••••••
Email	ghanghavnamita93@gamil.cc
DOB	09031993
Address	D1-303 madhuban buidling
City	titwala
State	maharashtra
Country	INDIA

Select Priority of colors 🟥 🟦 🟩 🟨 🟦 ⬛ 🟧

Fig VI.1:- Registration

Outputs are the most important and direct source in information to the consumer and administrator. Intelligent output design will improve the system's relationship with user and help in decision making. It has a conversation panel to display the connection information, remote messages and information for user. Efficient, intelligent output design should improve the system's relationship with the user and help in decisions making. It has conversation panel to display the connection information, remote message and information user.

Efficient, intelligent output design should improve the system relationship with the user and help in decision making. Since the report are directing referred by the management for a taking decision and to draw conclusion they must be design with almost care and the details in the report must be simple, descriptive and clear to the user.



AUITHENTICATION1

Username namita

Password

1	2	3	4	5	6
7	8	9	0	A	B
C	D	E	F	G	H
I	J	K	L	M	N
O	P	Q	R	S	T
U	V	W	X	Y	Z

namita

Fig VI.2:- Authentication

VII CONCLUSIONS

The techniques that generates session passwords that are resistant to brute force attacks, dictionary attack and shoulder surfing This techniques creates grid for session password generation According to more security this scheme is ways better than rest of the other schemes These scheme are completely new to the user and the proposed authentication technique should be verified generally This techniques can be used for external authentication to connect the application to a database or also it can be used to provide security to any windows application.

REFRENCES

[1].R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication.

[2].Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical passwords".

[3].A. F. Syukri, E. Okamoto, and M.Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security G. E. Blonder, "Graphical passwords," in Lucent Technologies,

[4].HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant To Shoulder Surfing.

[5].S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and lontudinal evaluation of a graphical password system".

[6] Meng, Y. Designing click-draw based graphical password scheme for better authentication. In Networking, Architecture and Storage (NAS)

[7] Hu, W., Wu, X., & Wei, G. The security analysis of graphical passwords. In Communications and Intelligence Information Security

[8] Ma, Y., & Feng, J.Evaluating usability of three authentication methods in web-based application. In Software Engineering Research, Management and Applications

[9] Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. In Convergence and Hybrid Information Technology

[10] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. Authentication using graphical passwords: effects of tolerance and image choice.