Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4-STAGE GRAPHICAL PASSWORD AUTHENTICATION SCHEME FOR CLOUD

[1]K. GANGADHARA RAO, [2]R.VIJAYAKUMARI, [3]B.BASAVESWARA RAO

[1]Associate Professor, Department of Computer Science, Acharya Nagarjuna University, Guntur

[2]Assistant Professor, Department of Computer Science, Krishna University, Machilipatnam

[3]Systems Programmer, Department of Computer Science, Acharya Nagarjuna University, Guntur

E-mail: [1]kancherla123@gmail.com, [2]vijayakumari28@gmail.com, [3]bbrao@alu.ac.in

ABSTRACT

Cloud computing is the fastest growing part of IT industry as it provides dynamic and scalable services to the user in a cost-efficient way. Unfortunately, cloud is also vulnerable to various attacks as it is based on Internet. Cloud service providers offering different types of services delivered over the internet without any delay are governed by Service Level Agreements, which are entered between the vendor and the user. Authentication still remains an issue that is vulnerable to shoulder surfing, guessing attack and various types of other attacks. There is a need to have a proper password checking mechanism so that the degree of vulnerability in the process of authentication gets reduced. In this paper, an effort has been made to present a novice algorithm for the authentication process which totally alleviates the problems of shoulder surfing and guessing attacks. This algorithm works in four stages. If all the four stages are through successfully then one can access the cloud securely.

Keywords: *Authentication, Shoulder-surfing attack, Graphical Passwords, Cloud Security*

1. INTRODUCTION

Cloud computing is the buzz word of today's world. It enables on-demand access to computing and data storage resources that can be configured to meet unique constraints of the clients with minimal management overhead. The recent rise in the availability of cloud services make them attractive and economically sensible for clients with limited computing and storage resources who are unwilling and unable to procure and maintain their own computing infrastructure. The ever increasing need for computing power and storage accounts for the steady growth in popularity of companies offering cloud services. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud. From the past few decades, there has been very fast advancement in computing technology. Systems have been designed which have high resource handling capability, capacity and computing power. All these online activity require some type of authentication. Authentication means to verify the identity of the user, which means whether the person is same which he pretends to be. Traditionally, alphanumeric passwords have been used for authentication. While today other methods including biometrics and smart cards are possible alternatives, passwords are likely to remain dominant for some time because of concerns about reliability, privacy, security, and ease of use of other technologies [15]. But, the use of textual passwords has significant drawbacks [12]. Because it is difficult for humans to remember random strings, users tend to ignore requirements for secure passwords. This leads to poor passwords practices, including short, simple passwords that are easy to break either by a dictionary attack or personal knowledge of the password owner, use of the same password over months or years, reuse of identical or nearly identical passwords on multiple systems, and tendency to write down passwords and store them insecurely, e.g., a text file containing the user's passwords stored on insecure computers or mobiles, post its notes stuck on or near the computer monitor or inside a desk drawer[16,17,18,19,20,21].

In an effort to improve password security by making passwords easier to remember, researchers have developed graphical passwords [3]. In a typical graphical password scheme a user chooses several images to be his or her password. When logging in, the user must click on the password images among a larger group of distracter images.

If the user clicks on the correct images, he or she is authenticated. User's memory for graphical password may be better than an alphanumeric password. Secure alphanumeric passwords (i.e., random strings) are based on pure recall from memory, a skill that is notoriously difficult for humans. By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. Indeed, image-based passwords have shown good memorability in user testing [15, 22, 23, 24, 25, 26].

However, the problem of shoulder surfing is a recognized drawback of graphical passwords [4, 5, 6, 7, 8, 9]. Shoulder-surfing refers to someone watching over the user's shoulder as the user enters a password, there by capturing the password [13]. While alphanumeric passwords systems are vulnerable to shoulder surfing if the attacker can see the keyboard, graphical password systems may be more vulnerable in certain settings. For example, clicking on images on a large, vertical display screen may make users' actions easier to capture. Some of the graphical password schemes are more time consuming to login and occupies large memory to store images [4, 10].

In this paper we introduce recognition based graphical password scheme based on [10] that is resistant to shoulder-surfing. It uses alphabets in place of images and works in four stages. By making use of alphabets when comparing with images, the storage space, loading time of the images will be minimized. The login screen at every stage is filled with characters from the 96 characters set in a random fashion. This randomization phenomenon of login screen keeps the shoulder surfer in a perplexed state.

This paper is organized as follows: in section II, related work is discussed; in section III, a new graphical password authentication scheme for cloud is introduced; in section IV, the algorithms for the proposed scheme is discussed and the flow charts for the proposed scheme are depicted; usability and security aspects of the proposed scheme are discussed and analyzed in section V, finally, the conclusion and future work are proposed in section VI.

2. RELATED WORK

In 1996, Blonder et al. [8] proposed a graphical password scheme, in which user has to create a password by clicking on different points on the image. At login phase, he has to locate those points correctly and click on them. This system is vulnerable to shoulder surfing.

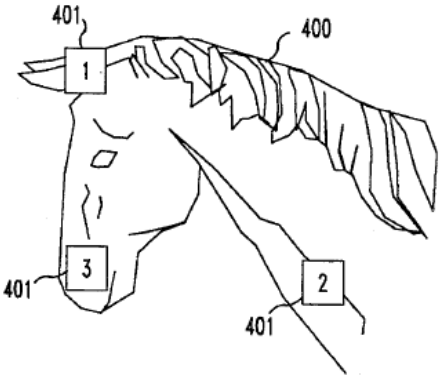


Fig : G.E.Blonder's Scheme [8]

Movable Frame Scheme, the intersection scheme, and triangle scheme are the three shoulder surfing resistant password schemes proposed by Sobrado and Birget [4] in 2002. In movable frame password scheme, the password picture of the user is located in the frame. The user has to create an invisible straight line such that the line connects the entire picture password. The user has to intersect all the pass images in the intersection scheme. The user has to choose and memorize several pass icons and his password in triangle scheme. This scheme is complex and tiresome and also consumes time.

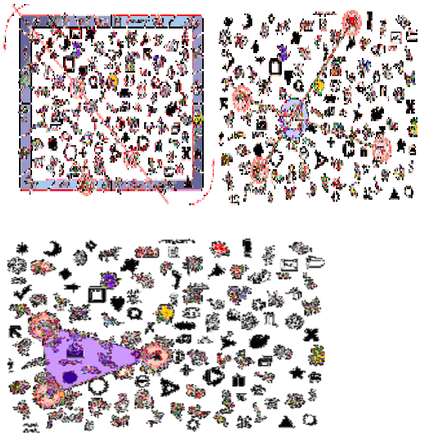
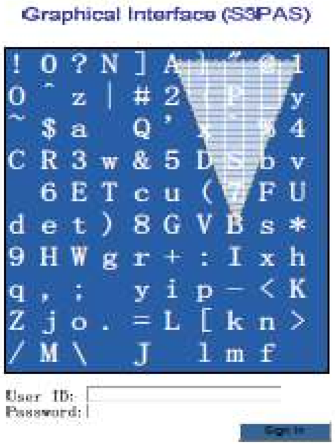


Fig 2: Shoulder surfing resistant graphical password schema [4]

In 2005, Real User Corporation proposed a technique called "PassFace" [9]. In this, user has to select four images containing human faces as his password at registration time. During login he will be provided with 3x3 grid consisting of 9 faces. Among which one is the passface and the eight are decoy faces. User has to identify that passface correctly and the process repeats for several times. If the user, correctly identifies all the passfaces, he is authenticated. These systems were highly vulnerable to shoulder surfing attack. Passface systems are easily anticipated as they are affected by race, gender and attractiveness.

Fig3 : Passfaces Scheme [9]

Huyanyu Zhao et al. [10] proposed a text-based shoulder surfing resistant graphical password scheme in 2007. In this scheme, the user is provided with a session password which is devised basing on several clicks inside the invisible pass triangles. The pass triangles are formed basing on the alpha numeric characters taken from the registered password, three at a time. The devised session password is used to login to the system. The login procedure of this scheme is very complex and tedious. It takes longer time to login.



Graphical Interface (S3PAS)

Fig 4: S3PAS Scheme [10]

Yamamoto et al. [7] proposed a shoulder surfing resistant graphical password scheme TI-IBA in 2009. In this scheme, user is given four slide shows at login time. He has to select one from them such that it contains the registered password image(s). The proposed system in this scheme was less constraint by screen size. So, it was easy to find out pass icons. But this system was vulnerable to accidental login. It is very difficult for the user to memorize and recognize the pass pictures during log in.

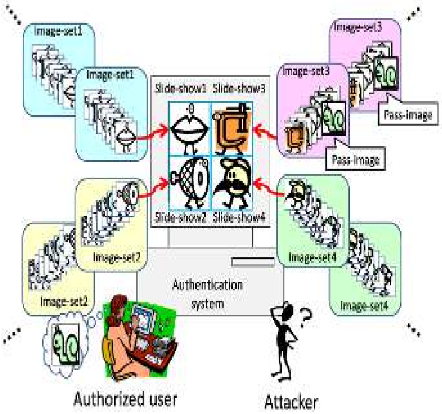


Fig 5: Another shoulder surfing resistant authentication system [7]

In 2011, Sreelatha et al. [11] proposed a text based graphical password scheme using colours. User has to remember and memorise the colors to be authenticated in this scheme. So, it was less effective.

In 2014, Shraddha M Gurav et al. [2] proposed a scheme for securing the cloud by means of image password. During registration, a set of images will be given to user, based on some calculations on the username. User has to select two images from them and two images will be given from server side. It forms full password and is stored in the database. To login to the system, user has to enter user name and identify the pass pictures appropriately and click on them to get access to the cloud.

Sumit H. Wagh and Aarti G. Ambekar[1] proposed a shoulder surfing resistant text based graphical password scheme in 2015. The login screen in this scheme consists of a circle and is divided into six sectors. Each sector contains twelve characters. User has to register his password and sector at registration time. During login, he has to rotate the sector containing the pass character into his designated sector, and then confirms it. He repeats it for 'L' number of times where 'L' is the length of the password. After finishing all the passes, user is allowed to access the system. This system is a bit confusing for the normal user.

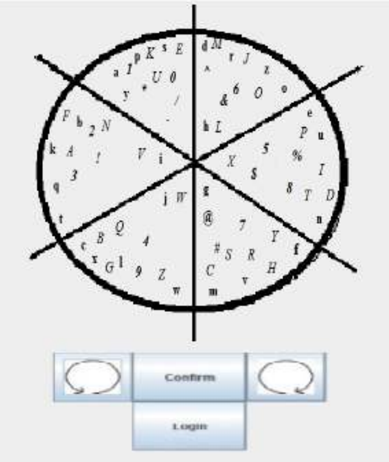
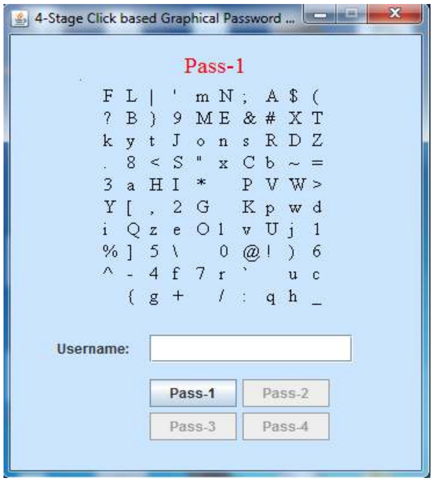


Fig 6: Shoulder surfing resistant text based graphical password scheme [1]

3. PROPOSED WORK

In this section, a novice shoulder surfing resistant namely "4-stage graphical password authentication scheme for cloud" is proposed. A user can compose his textual password of length four characters from 94 characters set. The password should be strictly of length four and all the four characters should be distinct. The password character set consists of 26(A-Z) upper case letters, 26(a-z) lower case letters, 10(0-9) digits and other 32 printable special characters from keyboard as specified by Huyanyu Zhao et al [10]. The login screen consists of 10x10 matrix in which 100 characters can be displayed as shown in Fig 7. Out of hundred locations in the matrix, ninety four locations are filled with distinct printable characters from password character set and other six locations are filled with spaces. At each phase of login, of a user, the location of characters in the interface are randomized.



Pass-1

F	L	|	'	m	N	;	A	$	(
?	B	}	9	M	E	&	#	X	T
k	y	t	J	o	n	s	R	D	Z
.	8	<	S	"	x	C	b	~	=
3	a	H	I	*		P	V	W	>
Y	[	,	2	G		K	p	w	d
i	Q	z	e	O	l	v	U	j	1
%	]	5	\		0	@	!	)	6
^	-	4	f	7	r	`		u	c
	{	g	+		/	:	q	h	_

Username:

Fig 7: Login screen (Phase wise randomized) for proposed Scheme

The proposed scheme has two phase working mechanism – Registration phase and Login phase. In registration phase, the user has to register by giving his username and selecting a password. The selected password is shifted circularly to the right by one character and stored in the database. For the login phase, the proposed algorithm gets processed in four stages. The user has to pass in each and every stage by entering the input. The input at any stage is given by clicking on the characters of the grid on the interface. At each stage, user has to click for three times for providing the input. If the input matches with the expected value then he is allowed to go to next stage. This process repeats for three times for three stages respectively. At the fourth stage, if the input matches with the expected value he is allowed to access the cloud resources. At any stage, if the input doesn't match with the expected value the user is rejected to access the cloud.

During the login process, the user has to provide four strings during four stages by clicking on the interface. Each and every string is of length three characters. At any stage, the user clicks on the interface for three times. The characters at those clicked locations are taken in sequence and a string of length three characters is formed with them. Therefore, for four stages four strings are generated by the user. Those strings are checked with the substrings of the password string, existing in the database.

Suppose that the registered password of the user is "i%>R". It is stored in the database by shifting the password circularly to right, by one character. i.e., the password stored in the database will be "Ri%>". Then at stage one, the password stored in the database is taken and rotated circularly by shifting one character to the left. First three consecutive characters from the left shifted password are taken and compared with the password entered by the user at this stage. If the entered password by the user matches with the substring, then he is allowed to go to the next stage. This process repeats for four stages by increasing the number of circular left shifts of the password. In stage two, the password is rotated circularly by shifting one character to left for two times; in stage three, it will be for three times and in stage four, it will be for four times. After passing stage four, the user is allowed to access the cloud resources. If the user fails to produce correct password string at any stage, then the login process will be terminated automatically and the user has to start again afresh.

During inputting of password by the user at any stage, the character is extracted from the clicked point on the grid. The tolerance area of the clicking point to extract the character is limited and it is only twelve. So the user has to click on the character very carefully. The slight deviation in clicking the character will give wrong result. Therefore, only the person who knows the password is able to click on the characters correctly. In that way, this algorithm prevents attacks by the intruders.

4. ALGORITHMS AND FLOWCHARTS

4.1 Algorithm for Registration

```
Step-1: Start
Step-2: Choose the password of length four at registration time
Step-3: Rotate the password circularly by shifting one character to the right
Step-4: Store the circularly rotated password in the database
Step-5: Stop
```

4.2 Algorithm for Login

```
Step-1: Start
Step-2: Enter username
Step-3: The saved password for the entered username is retrieved from the database and is kept
        in a string named “pwdstr”
Step-4: n=1
Step-5: User makes the login attempt by selecting three characters through clicking on the
        interface for 3 times.
Step-6: Rotate the password string, “pwdstr” circularly, by shifting one character to the left, by
        ‘n’ number of times and then extract the first three consecutive characters as a substring
Step-7: Compare the substring with the input given by the user at this particular stage

Step-8: If the substring matches with the entered password then
            Compute, n = n+1
        Otherwise
            Goto Step-10

Step-9: If n<= 4 then,
            Goto Step-5
        Otherwise
            display message “Login Success!!!” and allow the user to use cloud services
Step-10: Stop.
```

4.3 Flowchart for Registration

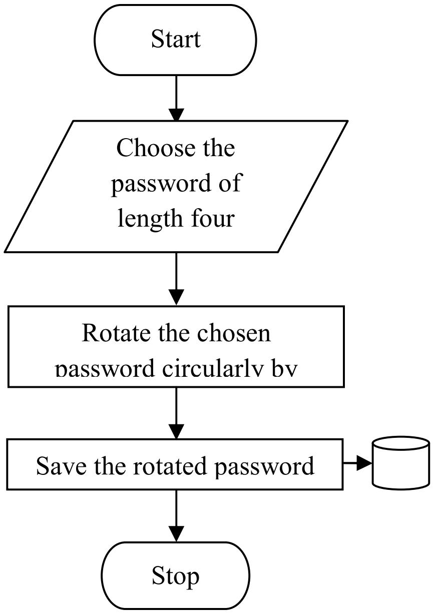

Start
Choose the password of length four
Rotate the chosen password circularly by
Save the rotated password
Stop

Fig 8: Flowchart for Registration Process

4.4 Flowchart for Login

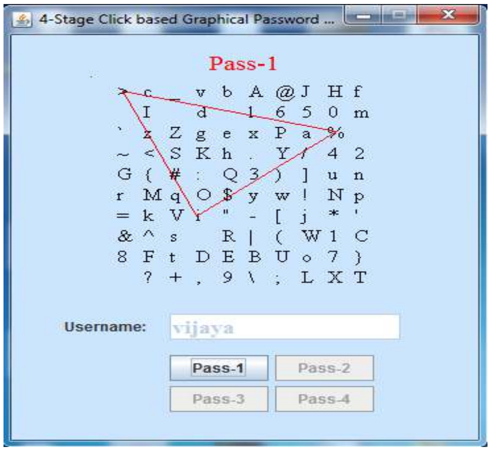
Flowchart for login procedure is displayed in Fig 9.

4.5 Login Procedure For Proposed Scheme

The login procedure for the proposed scheme is presented here with the help of an example. Suppose that the password registered by a particular user “vijaya” is “i%>R”. The user “vijaya” has to produce four substrings of the password registered, such as “i%>”, “%>R”, “>Ri”, and “Ri%” as input strings during four phases respectively.

Step-1

Initially, the login screen displays username field along with four buttons considering Pass-1, Pass-2, Pass-3, and Pass-4. Pass-1 button will be in the enabled mode initially. Other three buttons will be in disabled mode. User enters the username and has to locate three pass characters precisely on the interface and click on them, for the first phase.



Pass-1

```
> c _ v b A @ J H f
  I   d   1 6 5 0 m
` z Z g e x P a %
~ < S K h . Y / 4 2
G { # : Q 3 ) ] u n
r M q O $ y w ! N p
= k V r " - [ j * '
& ^ s   R | ( W 1 C
8 F t D E B U o 7 }
  ? + , 9 \ ; L X T
```

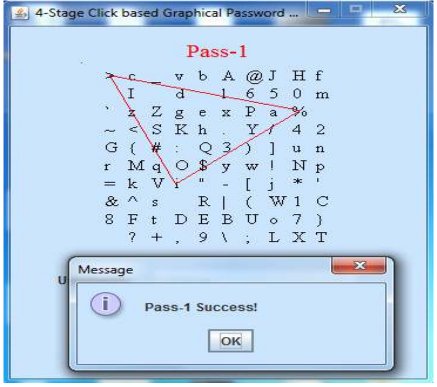
Username: vijaya

Fig 10: Selected Characters In Proposed Schema At Phase-1

In pass-1, username is entered and three pass characters are selected by the user as shown in Fig 10.

Step-2

Characters from the three clicked positions are extracted into a string variable. Another string variable contains substring of original password taken from database. These two are compared. If the clicked password matches with the substring then a success message is displayed and the user is allowed to go to pass-2.



Pass-1

```
> c _ v b A @ J H f
  I   d   1 6 5 0 m
` z Z g e x P a %
~ < S K h . Y / 4 2
G { # : Q 3 ) ] u n
r M q O $ y w ! N p
= k V r " - [ j * '
& ^ s   R | ( W 1 C
8 F t D E B U o 7 }
  ? + , 9 \ ; L X T
```

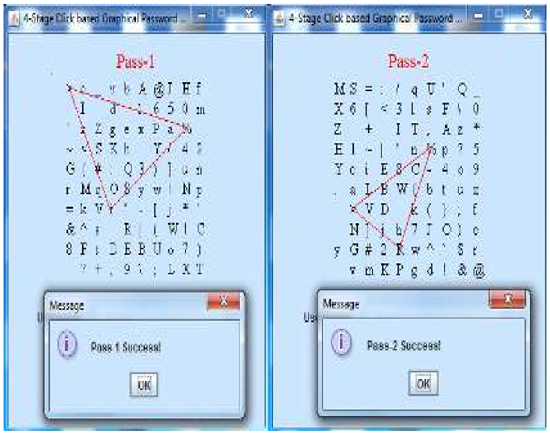
Pass-1 Success!

Fig 11: Success At Phase-1 In Proposed Scheme

The three pass characters entered by the user are "i%>" and is matching with the expected input. So, the user is allowed to go to step-2 automatically, by indicating success in Pass-1 as shown in Fig 11.

Step-3

In this step, pass-2 button will be in enabled mode. Click on the login interface for three times to produce a password for this stage.


4-Stage Click based Graphical Password ...
4-Stage Click based Graphical Password ...
Message
OK
Message
OK

Pass-1

```
> c _ v b A @ J H f
  I   d   1 6 5 0 m
` z Z g e x P a %
~ < S K h . Y / 4 2
G { # : Q 3 ) ] u n
r M q O $ y w ! N p
= k V r " - [ j * '
& ^ s   R | ( W 1 C
8 F t D E B U o 7 }
  ? + , 9 \ ; L X T
```

Pass-1 Success!

Pass-2

```
M S = : / q U ' Q _
X 6 [ < 3 l s F \ 0
Z   +   I T , A z *
E l - | ' n % p ? 5
Y c i E 8 C - 4 o 9
  a L B W \ b t u z
  > V D   & ( ) ; f
  N ] i b 7 I O ) c
y G # 2 R w ^ ` $ r
  v m K P g d ! & @
```

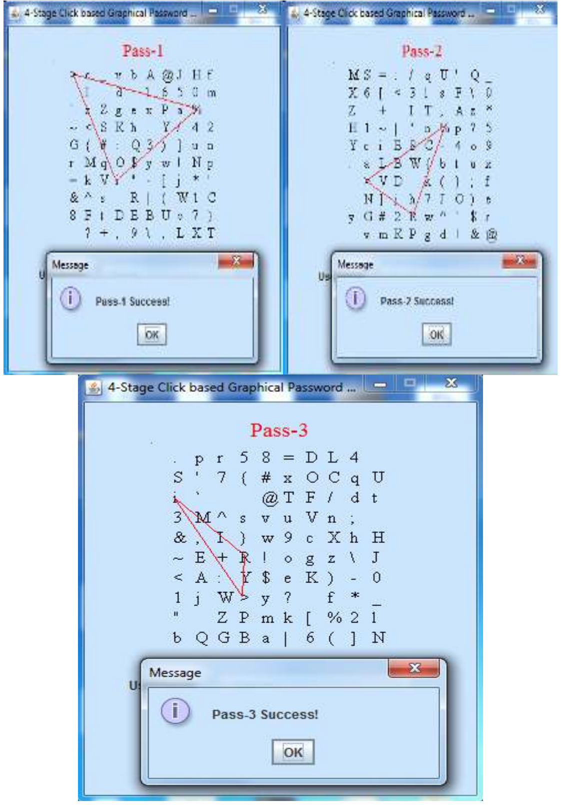
Pass-2 Success!

Fig 12: Success At Phase-2 In Proposed Scheme

The three pass characters entered by the user at this stage-2 are "%>R" and is matching with the expected input. So, the user is allowed to go to step-3 automatically, by indicating success in Pass-2 as shown in Fig 12. The success in this step indicates that pass-1 is success and pass-2 is success.

Step-4

In this step, pass-3 button will be in enabled mode. Click on the login screen for three times to generate a password for phase-3.


4-Stage Click based Graphical Password ...
4-Stage Click based Graphical Password ...
4-Stage Click based Graphical Password ...
Message
OK
Message
OK
Message
OK

Pass-1

```
> c _ v b A @ J H f
  I   d   1 6 5 0 m
` z Z g e x P a %
~ < S K h . Y / 4 2
G { # : Q 3 ) ] u n
r M q O $ y w ! N p
= k V r " - [ j * '
& ^ s   R | ( W 1 C
8 F t D E B U o 7 }
  ? + , 9 \ ; L X T
```

Pass-1 Success!

Pass-2

```
M S = : / q U ' Q _
X 6 [ < 3 l s F \ 0
Z   +   I T , A z *
E l - | ' n % p ? 5
Y c i E 8 C - 4 o 9
  a L B W \ b t u z
  > V D   & ( ) ; f
  N ] i b 7 I O ) c
y G # 2 R w ^ ` $ r
  v m K P g d ! & @
```

Pass-2 Success!

Pass-3

```
. p r 5 8 = D L 4
S ' 7 { # x O C q U
i `     @ T F / d t
3 M ^ s v u V n ;
& , I } w 9 c X h H
~ E + R ! o g z \ J
< A : Y $ e K ) - 0
1 j W > y ?   f * _
"   Z P m k [ % 2 1
b Q G B a | 6 ( ] N
```

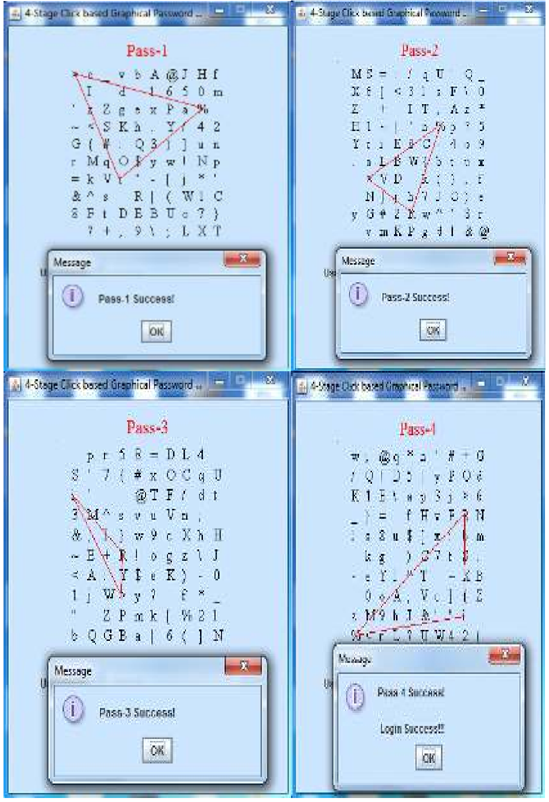
Pass-3 Success!

Fig 13: Success At Phase-3 In Proposed Scheme

The three pass characters entered by the user at this stage-3 are ">Ri" and is matching with the expected input. So, the user is allowed to go to step-4 automatically, by indicating success in Pass-3 as shown in Fig 13. The success in this step indicates that pass-1 is success, pass-2 is success, and pass-3 also is success.

Step-5

In this step, pass-4 button will be in enabled mode. Click on the login interface for three times to produce a password for phase-4.



4-Stage Click based Graphical Password ...

Pass-1

Message

Pass-1 Success!

OK

4-Stage Click based Graphical Password ...

Pass-2

Message

Pass-2 Success!

OK

4-Stage Click based Graphical Password ...

Pass-3

Message

Pass-3 Success!

OK

4-Stage Click based Graphical Password ...

Pass-4

Message

Pass-4 Success!

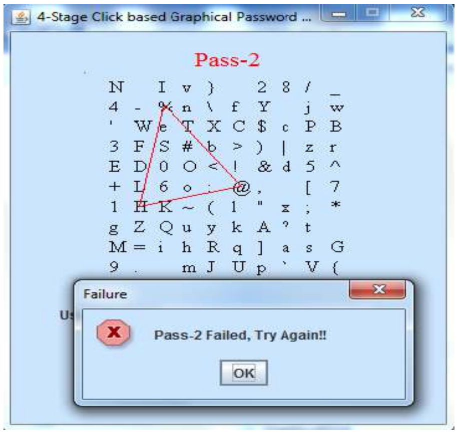
Login Success!!

OK

Fig 14: Ultimate Success At Phase-4 In Proposed Scheme

The three pass characters entered by the user at this stage-4 are "Ri%" and are matching with the expected input. So, the user is given a message saying that "Login Success!!!" as shown in Fig 14. The success in this step indicates that pass-1 is success, pass-2 is success, pass-3 is success and pass-4 also is success. Therefore, the user is granted permission to access the cloud.

If the user fails at any of the four passes he is banned to move further. The login screen displays failure message and disappears immediately. The user has to start over anew. Example failure message at stage two is shown below



4-Stage Click based Graphical Password ...

Pass-2

Failure

Pass-2 Failed, Try Again!!

OK

Fig 15: Example For Fail In Login Process, In Proposed Scheme

The expected input by the particular user "vijaya" at stage-2 is "%>R". But the input entered in the above Fig 15 is "%@H ". So, the user gets failure message and gets terminated from the login process.

If the user fails to produce correct password for 3 consecutive times the account will be disabled. In such case, a secret link will be sent to the user's registered mail-id through which he can re-enable his disabled account.

5. USABILITY STUDY AND SECURITY ANALYSIS

We have conducted a usability study in the lab with 28 participants out of which 13 were male and 15 were female with their ages ranging from 22 to 26. A learning session was conducted explaining the login procedure of the proposed click based graphical password scheme. Initially, they were trained explaining the click rules of the login interface at each and every stage. The results were encouraging that the trainee users were able to locate and click on the pass characters quickly and correctly. The login procedure took about 30 seconds on average using i5 processor.

In this section, we analyze the proposed scheme considering two parameters usability and security. The proposed system has 94 characters in the password character set. A valid password contains 4 distinct characters. Therefore, total number of all possible passwords is $94C_{4.}$ Hence, password space for the given scheme is $3.0495x10^{6.}$

The success probability of accidental login is called as password entropy. The login process contains four phases. At any phase, three distinct characters should be located and clicked on them. This procedure is same at all phases.

The probability of guessing first character at any stage is 1/94. The probability of guessing second character is 1/93. The probability of guessing third character is 1/92. If X is the probability of guessing pass characters at any phase, then X can be given as

$$X = \frac{1}{94} \times \frac{1}{93} \times \frac{1}{92}$$

If P1, P2, P3 and P4 are the probabilities of guessing pass characters at stage-1, stage-2, stage-3 and stage-4 respectively then,

The success probability at phase-1 can be given as, P1= 1.2433X10^{-6} i.e.,

$$P1 \cong 0.0000012433$$

Success probability at phase-2 is success at phase-1 and success at phase-2. Therefore, success at phase-2 is

$$P1 \times P2 = \left[\frac{1}{94} \times \frac{1}{93} \times \frac{1}{92} \right]^2$$

Success probability at phase-3 is given by

$$P1 \times P2 \times P3 = \left[\frac{1}{94} \times \frac{1}{93} \times \frac{1}{92} \right]^3$$

Success probability at phase-4 is given by

$$P1 \times P2 \times P3 \times P4 = \left[\frac{1}{94} \times \frac{1}{93} \times \frac{1}{92} \right]^4$$

If 'P' is the overall probability of the proposed scheme then, the value of P is nothing but the value of

$$P1 \times P2 \times P3 \times P4 = \left[\frac{1}{94} \times \frac{1}{93} \times \frac{1}{92} \right]^4$$

i.e.,

$$P \cong 0.000000000000000000000023900$$

All most a negligible value which means the probability of guessing a password by looking over the shoulders is impossible. The robustness of the proposed algorithm is 1-P. i.e., 1- 0.000000000000000000000023900 which is similarly equal to 0.9999999. Therefore, the proposed scheme is 99% secure.

6. CONCLUSION AND FUTURE WORK`

Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with problems. Authenticating a user to access cloud resources or services is one such problem. In case, somebody see a user entering the graphical password can easily remember or guess the password and can take access of the resources. Our major goal is to overcome this security issue through authentication scheme.

In this paper, we presented a graphical shoulder surfing resistant authentication scheme by taking cloud as a platform. Through this scheme, the user can efficiently and effortlessly complete the login process without being concerned about shoulder surfing attacks. From a security perspective, this exploration is anticipated to support the development of graphical passwords especially recognition based. Our research shows that the future developments in the field of recognition-based should concentrate on enriching the login time, usability and cognizability. So, a method for contracting the time gap in the authentication process and balancing usability will lead to better graphical password systems. Also, making these schemes available on all platforms is another area for future research.

REFERENCES

[1] Sumit H. Wagh and AartiG.Ambekar, "Shoulder Surfing Resistant Text-based Graphical Password Scheme", *Proc. of International Conference on Computer Technology*, 2015, pp.17-19.

[2] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "Graphical Password Authentication Cloud Securing Scheme", *International Conference on Electronic Systems, Signal Processing and Computing Technologies*, 2014, pp. 479 - 482.

[3] XiaoyuoanSuo, Ying Zhu, G.Scott. Owen, "Graphical Passwords: A survey", *Proc. of 21st Annual Computer Security Applications Conference (ACSAC 2005)*, Tucson, AZ, 2005.

[4] L.Sobrado and J.C.Birget, "Graphical Passwords", *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, Vol. 4, 2002.

[5] L.Sobrado and J.C.Birget, "Shoulder-surfing resistant graphical passwords", *Draft*, 2005.

[6] S.Wiedenbeck, J.Waters, L.Sobrado, and J.C.Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", *Proc. of Working Conference on Advanced Visual Interfaces*, May.2006, pp. 177-184.

[7] T.Yamamoto, Y.Kojima, and M.Nishigaki, "A shoulder surfing resistant image-based authentication system with temporal indirect image selection", *Proc. of the 2009 Int. Conf. on Security and Management*, July 2009, pp. 188-194.

[8] G.E.Blonder, Graphical Passwords. *United States Patent* 5559961, 1996.

[9] R.U.Corporation. *How the passface system works*, 2005.

[10]Huanyu Zhao andXiaolin Li, "S3PAS: A Scalable Shoulder –Surfing Resistant Textual-Graphical PasswordAuthentication Scheme", *Proc. of 21st International Conference on Advanced Information Networking and Applications Workshops*, Vol.2, May 2007, pp. 467-472.

[11]M.Sreelatha, M.Shashi, M.Anirudh, Md.SultanAhamer, and M.Manoj Kumar, "Authentication schemes for session passwords using colour images", *International Journal of Network Security and its Application*, Vol.3, No. 3, May 2011.

[12]A.Adams and M.A. Sasse, Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures, *Communications of the ACM,* 42:41-46, 1999. [13]Mirang Park, Yoshihiro Kita, KentaroAburada, Naonobu Okazaki, "Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance", *Proc. of 2014 International Conference on Network-Based Information Systems, 2014*, pp. 495-500.

[14] www.wikipedia.org

[15] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), People and Computers XIV – Usability or Else, *Proc. of HCI 2000, Springer*, 2000, 405-424.

[16] Adams, A. and Sasse, M.A. Users are not the enemy. *CACM 42*, 12 (1999), 41-46.

[17] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. Generating and remembering passwords. *Applied Cognitive Psychology*, 18, (2004), 641-651.

[18] Feldmeier, D.C. and Karn, P.R. UNIX password security –ten years later. In Advances in cryptography – CRYPTO'89, *Lecture Notes in Computer Science 435*, Springer-Verlag 1990, 44-63.

[19] Ives B., Walsh K. R. and Schneider H., 2004. The domino effect of password reuse. *CACM*, 47, 4(2004). 76-78.

[20] Morris R. and Thompson K. Password security: A case Study. *CACM*, 22, (1979), 594-597.

[21] Norman D.A. The Design of Everyday Things. *Basic Books*, New York, 1988.

[22] De Angeli A, Coutts M., Voventry L, Cameron D, Johnson G.I., and Fischer M., VIP: A visual approach to user authentication. *In Proc. Of AVI 2002*, ACM Press, NY, 2002, 316-323.

[23] De Angeli A, Coventry L, Johnson G., and Renaud K. Is a picture worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63, 1-2 (2005), 128-152.

[24] Dhamija R. Hash visualization in user authentication. *In proc. Of CHI 2000, ACM Press*, NY, 2002, 279-280.

[25] Dhamija R. and Perrig A. Déjà vu: User study using images for authentication. *In Ninth Usenix Security Symposium*, 2000.

[26] Wiedenbeck S, Waters J, Birget J.C., Brodskiy A., and Memon N. Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies,* 63, (2005), 102-127.

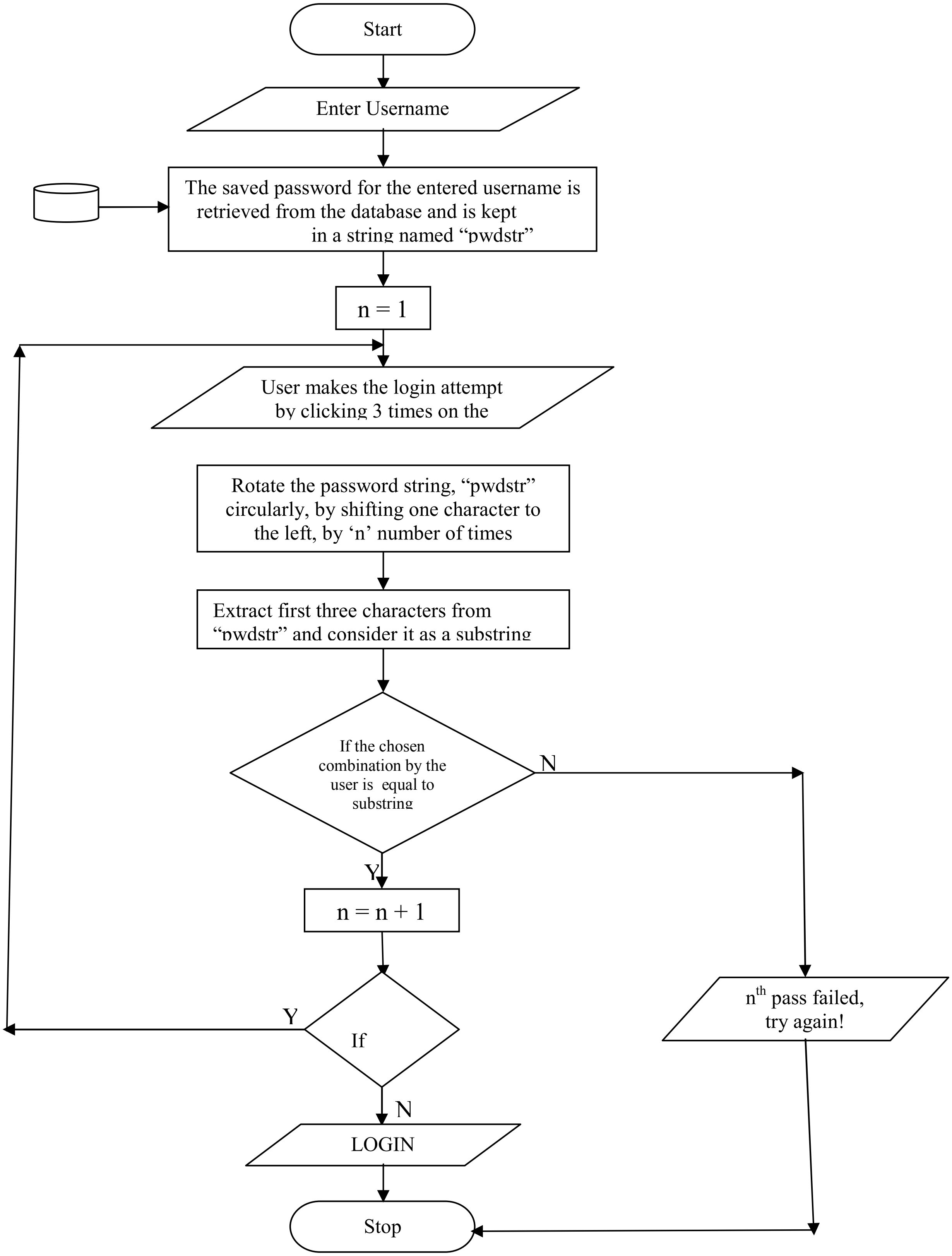

Start
Enter Username
The saved password for the entered username is retrieved from the database and is kept in a string named "pwdstr"
n = 1
User makes the login attempt by clicking 3 times on the
Rotate the password string, "pwdstr" circularly, by shifting one character to the left, by 'n' number of times
Extract first three characters from "pwdstr" and consider it as a substring
If the chosen combination by the user is equal to substring
N
Y
n = n + 1
If
Y
N
LOGIN
nth pass failed, try again!
Stop

Figure 9: Flowchart for Login