ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Multilayer Graphical Password Authentication

Sneha Sahare[#1], Prashant Chouragade[#2] , Ninad khonde[#3] , Kapil Dhopre[#4] , Sagar Shende[#5]

Professor, Dept. of CSE, Dr. Babasaheb Ambedkar College of Engineering and Research, Maharashtra, India[1]

B.E Student, Dept. of CSE, Dr. Babasaheb Ambedkar College of Engineering and Research, Maharashtra, India[2, 3, 4,5]

ABSTRACT: Nowadays computer system access uses alphanumerical password. Such password hard to remember due to its length (long) or sometime it is randomly generated. Short and simple passwords may lead to vulnerability as well as write password in text file and put it in insecure place (drawer) which is also highly vulnerable. To overcome it, we introduce passwords which make use of graphical,such as images. Humain brain are more supportive to pictures rather then text. So such password easy to remember to use.

KEYWORDS: Brute force attack, Dictionary Attack, Malware, Social Engineering.

I. INTRODUCTION

Authentication is the process of determining whether a user is authorized or not. Authentication mainly applied to system, website, files,folder etc. Traditional authentication include using alphanumerical password. But there are some drawback with it as vulnerable in most common attack like dictionary attack. Simple password are easy to remember but it leads to vulnerable situation where guessing password plays an important role. Complicated password are hard to guess as well as hard to remember as well. Sometime user write their password on paper and put it in drawer which is obvious insecure place

Biometric password may overcome such issues. But it is more complex and expensive. Psychological survey says that human brain more compatible with picture than the text. Graphical password scheme is less complex than the biometric.

In graphical password authentication technique, user is given with the set of images, Sequential click on images, Considered as password. The purpose behind graphical password is that images are more memorable. No need to use keyboard, Easy to work with it.

II. RELATED WORK

Authentication is very sensitive job.where authentication can be done in three ways.

1. Text password
2. Token as a password
3. Biometric

Text Base Password:- It is traditional way of authentication. This passwords are combination of alphabets,numerals or special symbol. This passwords are good if they are complicated and they contain minimum 8 character and necessarily contain special symbol.

The disadvantage of it include,hard to remember,easy to guess. Simple password mainly contain name date of birth which are easy to crack and complicated password which are long enough are hard to remember. Another major drawback is vulnerable to dictionary attack. In dictionary attack,all the possible sequence are applied in order to breach the security.

Biometric:-

This authentication is hard to spoof forge. Here biological characters are the authentication key biometric authentication goes with two ways. They are Physiological and Behavioral include shape of body like finger print, palm etc. Behavioral characteristics include voice most common used technique is fingerprints.

The disadvantages are cost. Device use by Biometric system are of high cost. It is complex and time consuming. Another major drawback is it breach by denial-of-service attack which will result in recognize authenticating person is authorize or vice versa.

Safety:- There are various attacks namely Brute force,Dictionary attack,Malware,Social Engineering. But according to research these attack does not make lead in case of graphical password

Brute force attack:-

Attacker try each and every passwords sequence by guessing until correct passwords found. Graphical passwords are less affected by these attack as password space is 94^N where N=number of character in passwords and 94 is number of printable characters,As many passwords images give high space.

Dictionary Attack :-

Here dictionary of every possible string is referred to breach the password. Graphical password are safe in this case as it contain password in term of mouse click. So Graphical password are less vulnerable in this attack.

Malware:-

` In this attack a special software capture the keyboard motion but in case of graphical password capturing motion of mouse is not enough.

Social Engineering:-

In this case of attack, Psychologically user get manipulated by attacker. But having graphical password, user put away from such situation.

III. Proposed plan

The main purpose of "Multilayer Authentication password" is to provide multilayer password security which is based on graphics. The layer contains four modules.

First module contain the single image and the multiple points have to be selected from that image which will verify at the time of authentication.

Second module contain the multiple image and single point from each image have to be select which will verify at the time of authentication.

In Third module the pattern to be form which will user has to drawn at the authentication time And the fourth module contain to select the security question and the answer it. If user forget the password then these module helps for accessibility.

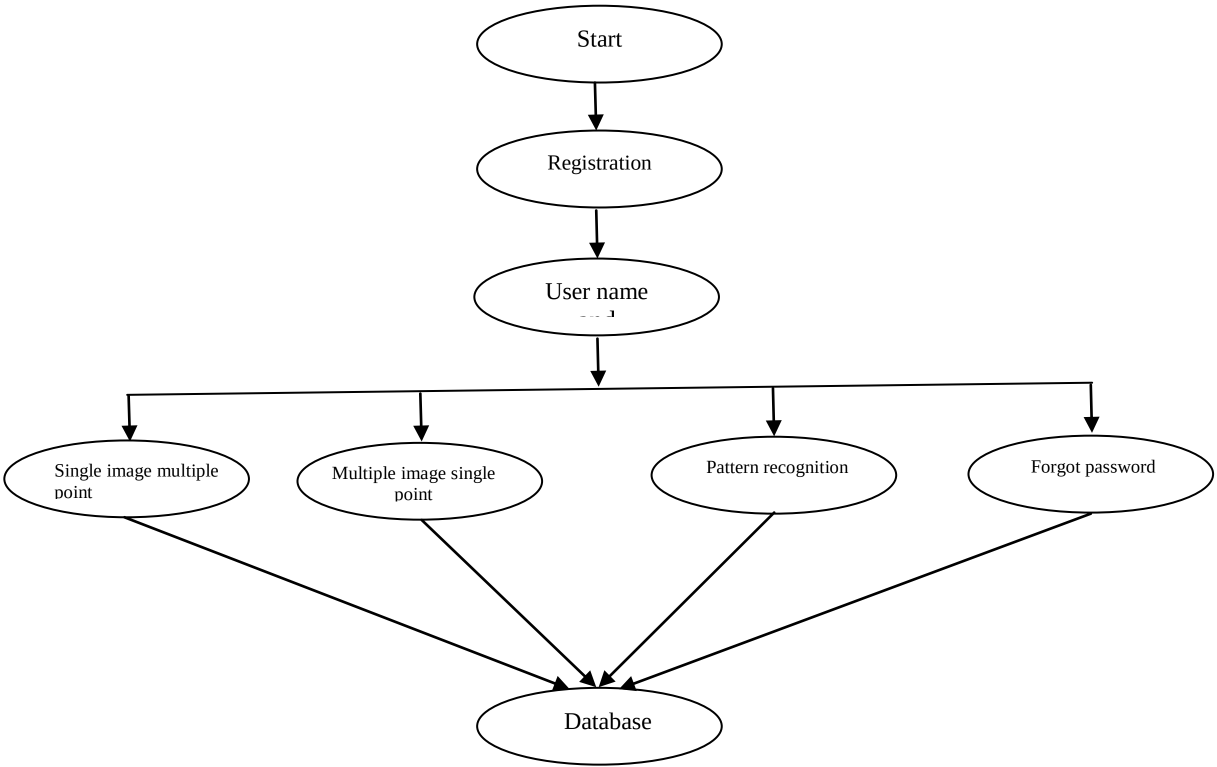
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

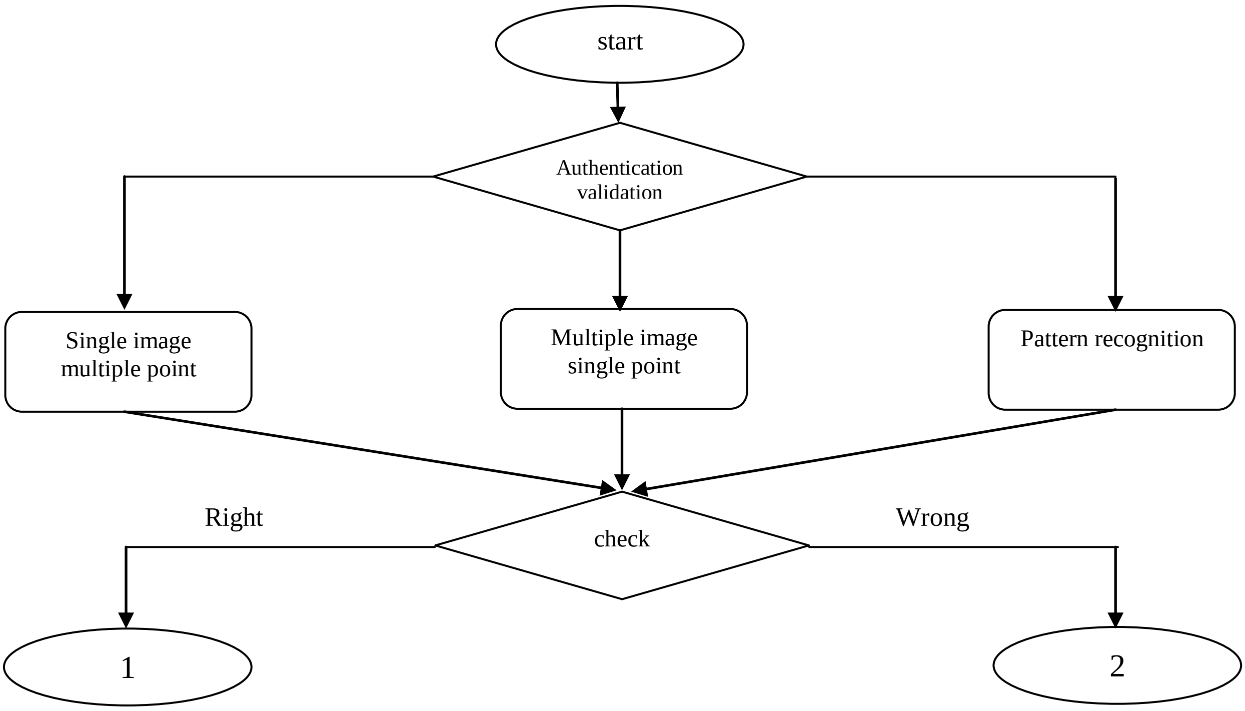
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017



Fig(1) Flow chart for Registation


start
Authentication validation
Single image multiple point
Multiple image single point
Pattern recognition
Right
check
Wrong
1
2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

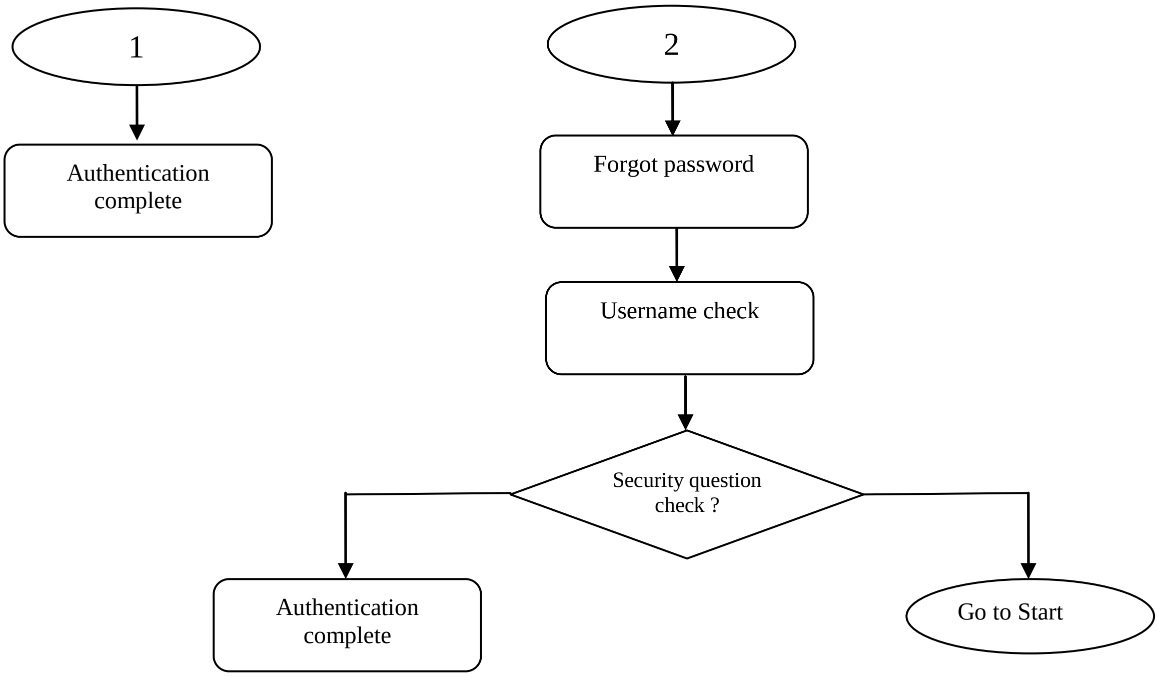


Fig (2) flow chart for user login

IV. SIMULATION RESULTS

The two mode are available to user, first one is registration and the second one is authentication(login).

The registration phase, user have a 3 choice and the recover password (forgot password). The three phase are included 3 method respectively. Which are described below. In first method,one image has to select by user, number of point to be click on the image has to be selected. At the second method multiple image to be select and click single point on each image. At the third method user will make a pattern. And lastly for the security purpose user will select security a question by your satisfying answer.

The login phase, user will select each method on his search. And he has to solve it with the help of solution he uses at the registration phase. Each solution will cross verify with the registration time solution . If solution is appropriate then user will get access.

And if user forgot the solution of the method he chooses at registration phase then security question will be helping hand for the user. User has to correctly answer the question he choose at registation phase.

V. CONCLUSION AND FUTURE WORK

Text password are widely used authentication yet. But Text based password are vulnerable in term of security. Another more secure ways of authentication as compare to text base password is graphical password. But graphical password are less aware. Graphical password tends to click point an image and make a pattern which takes place of typing textual password graphical password are able to resist Brute Force Attack, Dictionary Attack,Social Engineering are malware etc. Graphical password still not in use because it requires large storage space and time consuming.

REFERENCES

1. Prashanthi muddam , D.Raman “Graphical Password Authentication ”, *International Research journal of Engineering and Technology*, volume:03 Issue : 08,August-2016.

2. S.M. Furnell et al., "Authentication and Supervision: A Survey of User Attitudes." ,Computers & Security, vol.19 no.6, pp 529-539, 2000.
3. Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" ,In Proceedings of the 9th USENIX Security Symposium, August 2000.
4. D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies." IJCSNS, vol. 10, no.4. April, 2010.
5. Er. Aman kumar ,Er Naveen Blandi. "A Graphical password Based Authentication Based system for mobile devices", International Journal of computer science and mobile computing ,vol 3 Issue 4, April -2014. Pageno.744-754.
6. A. Jain, L. Hong, and S. Pankanti, "Biometricv identification," Communications of the ACM, vol. 33,pp. 168-176, 2000.
7. A. Gilbert, "Phishing attacks take a new twist," in CNET News.com, May 04, 2005.
8. M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.
9. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
10. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
11. R.J. Sutton, Secure Communications: Applications and Management. Chichester: John Wiley & Sons, Ltd. 2002.
12. Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04.

BIOGRAPHY

Prof.Sneha Sahare is working as a Professor, Department of Computer Science And Engineering of Dr.Babasaheb Ambedkar College of Engineering and Research.

Mr.Prashant Chouragade: Researcher, Department of Computer Science And Engineering of Dr.Babasaheb Ambedkar College of Engineering and Research.

Mr.Ninad Khonde: Researcher, Department of Computer Science And Engineering of Dr.Babasaheb Ambedkar College of Engineering and Research.

Mr.Kapil Dhopre: Researcher, Department of Computer Science And Engineering of Dr.Babasaheb Ambedkar College of Engineering and Research.

Mr.Sager Shende: Researcher, Department of Computer Science And Engineering of Dr.Babasaheb Ambedkar College of Engineering and Research.