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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

A Shoulder Surfing Resistant Graphical Authentication System

Pallavi Jha, SupriyaPhapale, Dhanshree Khopade, Nitin Kale, Mayur Murumkar

Asst. Professor, Dept. of C.E, Siddhant College of Engineering, Sudumbare, Pune, India

B.E Student, Dept. of C.E, Siddhant College of Engineering, Sudumbare, Pune, India

B.E Student, Dept. of C.E, Siddhant College of Engineering, Sudumbare, Pune, India

B.E Student, Dept. of C.E, Siddhant College of Engineering, Sudumbare, Pune, India

ABSTRACT: Confirmation in view of passwords is utilized generally in applications for PC security and protection. Be that as it may, human activities, for example, picking awful passwords and contributing passwords in an uncertain way are respected as the weakest connection in the validation chain. As opposed to subjective alpha-numeric strings, clients have a tendency to pick passwords either short or significant for simpler intention. With web applications and portable applications heaping up, individuals can get to these applications whenever and any place with different gadgets. This advancement brings incredible accommodation yet additionally builds the likelihood of presenting passwords to bear surfing assaults. Aggressor or scan watch specially or utilize outside chronicle gadgets to gather client qualifications. To defeat this issue, here development of a novel verification framework Pass-Matrix, in light of graphical passwords to oppose bear surfing assaults. With on-time substantial log in marker and calculative level and vertical bars covering the whole extent of pass-pictures, Pass-Matrix had no insight for aggressors to make sense of or limit the secret key even they direct different camera based assaults. Likewise actualized a Pass-Matrix model on Android and did genuine client analysts assessor tsm mobility and ease of use. From the trial result, the proposed framework accomplishes better imperiousness to bear surfing assaults while looking after ease of use.

KEYWORDS: Energy efficient algorithm; Graphical Passwords, Authentication, Shoulder Surfing Attack.

I. INTRODUCTION

A graphical password is one of the best and simple methods of remembering password in terms of photo and images and etc. It is a kind of authentication that behaves like as authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. As we know graphical user interface is a kind of image shuffling approach and instead of many here we can also say this as a graphical password authentication. A graphical password is easier than a text-based password for most people to remember. Assume about 8-character pwd if necessary to take some advantages over particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a globe of the world), the city of Nice (from a globe of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle as per the international map shown.

As in current scenario we seen around us the uses of graphical password authentication are increasing a lot. Also it provides better security and easy to remember instead of complex password reading. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. Hence we require 100 images on each of the 8 pages in an 8-image password, instead of 1008, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.

DOI: 10.15680/IJIRCCE.2017. 0510055

II. RELATED WORK

Basically graphical user authentication is based on three criteria as we discussed below:

i. A Secure Recognition Based Graphical Password by Watermarking. ... There is an alternative solution to the text-based authentication which is the GUA (Graphical User Authentication) or simply Graphical Password based on the fact that humans tend to remember images better.packet has passed through.Proposed algorithm.

ii. Pure Recall Based graphical password in which we see icon based image selection and authentication which is quite important and more beneficial and secure than others. Basically introduced in 1999 but cannot implement that time and successfully implement in 2007.

iii. Cued Recall-Based Technique in this technique gesture based authentication will be possible and in it we guess our probability based password.

GOALS AND OBJECTIVES:-

Graphical password is the secured password system, different than traditional text Password system in which user need to select Pass-Matrix. It is difficult to crack the graphical password. So the system is secured.

III. EXISTING SYSTEM

Now in today's market smart phone is one of the great digital marketing hubs which consist of Graphical password. This may come from selfie era also in which 90.23% of the world population has been engaged in this prophesion so it is quite simple to load one image and take something from it and use it as a security and there is lot problems will faced by small co-operates companies and also even by big companies facing security problems but they pays a lots of money on it. As we seen our case study now a days no company utilize their own DB for storing your personal directory hence they decided to take the personal DB under cloud authentication for better communication and security. Now a days the password system using graphics and images provides our security environment.

IV. ARCHITECTURE

As we seen in the below diagram as we discussed earlier about graphical password pattern in which we adopt one image and take one part from it for password and this part is going to save into a DB for further process.
So let us see the diagram and listed some of the important point below:-

It consist of user which is the 1st part of our concern who will going to set one image based graphical password for security and then it is transmitted for authentication at admin part and then the overall data of the secure password authentication will be loaded into a DB from which user retrieve their user password any time as they require.

The whole system is lies on security on warfare for providing security at very best.

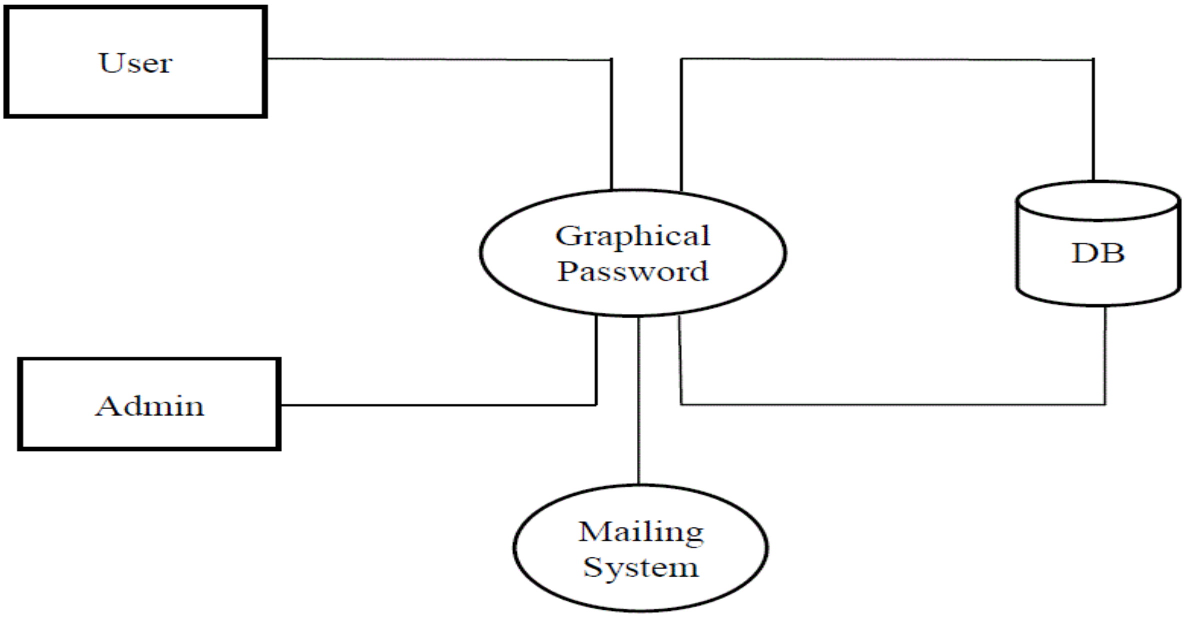

Figure 3. System Architecture of Persuasive Graphical Password System

As we seen above the whole scenario about password security and authentication around the different user device like android, windows, and also tab…..

V. PROJECT RELEVANT MATHEMATICS

SYSTEM DESCRIPTION:-CREDIT CARD FRAUD AND PERSONAL INFORMATION SECURITY ARE MAJOR CONCERNS FOR CUSTOMERS AND BANKS ESPECIALLY IN THE CASE OF CNP (CARD NOT PRESENT).
LET S BE A SYSTEM THAT DESCRIBES PAYMENT GATEWAY SYSTEM S = IDENTIFY INPUT AS I S = I,..
LET I = I1, I2, I3, ..ID THE INPUT WILL BE ACCOUNT NUMBER AND PASSWORD
IDENTIFY OUTPUT AS O S = I,O, O = CA WILL SENDING.
THE CONFIRMATION AFTER USER AUTHORIZATION.
IDENTIFY THE PROCESSES AS P S = I, O, P,.. P = E, D E=PARAMETER, USER ID,
PASS-MATRIX POINTS D=PARAMETER, USER AUTHORIZED, PASS MATRIX POINTS VERIFICATION
IDENTIFY FAILURE CASES AS F S = I, O, P, F,. F=FAILURE OCCURS WHEN THE CA IS VERIFIED UNAUTHORIZED USER.
IDENTIFY SUCCESS AS S. S = I,O,P,F,S, S=WHEN CA IS VERIFIED BY AUTHORIZED USER.
IDENTIFY THE INITIAL CONDITION AS I C S = I, O, P, F, S, I C, I C=PASS-MATRIX POINTS. MUST BE REQUIRED TXN.

VI. HARDWARE REQUIREMENT

a) SYSTEM PENTIUM IV 2.4 GHZ
b) HARD DISK 40 GB
c) FLOPPY DRIVE 1.44 MB
d) RAM 512MB

VII. SOFTWARE REQUIREMENT

a) SOFTWARE RESOURCES REQUIRED
b) OPERATING SYSTEM: WINDOWS XP/7/8/8.1
c) IDE: ECLIPSE

d) PROGRAMMING LANGUAGES: JAVA
e) DATABASE: ORACLE
f) WEBSITE SERVER: ORACLE SERVER

IX. CONCLUSION AND FUTURE WORK

In the current scienario there are many authentication schemes are revolving around the world. If they are categorized based on usability and security then most of them fall into the category of security that ensures the safety of the users account using second factor, but they lack proper usability. The remaining are the authentication schemes that are designed to achieve better usability, but lack proper security to protect the user from communication channel attacks and masqueraded server attacks. This research was aimed at providing authentication schemes that shall bridge the gap between security and usability. The main motive of using graphical method is around more security with easy password remember motive. The work started with the survey of current research in smart card based Two-Factor Authentication schemes that resulted in identifying various schemes on dynamic ID.

These schemes generate a dynamic ID at each user login, thus resisting the threat of identity theft. Though the security analyses of the schemes were presented through theoretical intuition, but none of them were evaluated for security using formal methods. Moreover, most of these schemes are found to be vulnerable to - 220 -the common authentication attacks such as Replay Attack, Guessing Attack, Stolen Verifier Attack, In-sider Attack, Server Spoofing Attack etc. Therefore, an enhanced dynamic ID based scheme was proposed that provides better security strength comparing to existing schemes.

As we see the existing and the proposed is not more different but proposed has some prior steps towards the existing. To validate the claims the security analysis of the scheme was presented, proposed scheme is also implemented alongside other proposed scheme.Text-o-Graphic Password which is completely based on Authentication based Scheme: While it is used in designing the Graphical Password Scheme, it was found that the recognition based graphical password could be susceptible to guessing, therefore, to overcome this; a novel graphical password called text-ographic password with two variations namely S-27 and S-16 was proposed. The user password in text-o-graphic method is the combination of image and its tag. S-27 presents three grids (each having nine images) to the user for password selection. The user has to choose one image from each grid and write a description called tag about the image so that the concatenation of three images along with their tags makes the users password. S-16 presents one grid of sixteen images of which the user has to choose one image and associate a tag to it.

REFERENCES

1. B.Hema , Assistant Professor / IT R.Manikandan , J.Vignesh ,S.Venkatesan,B.Tech / IT VelammalInsitute Of Technology, Chennai,fundamental security on cloud , IRACST - International Journal of Computer Science and
Information Technology Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No2, April 2015.
2. KavithaMurugesan, ShilpaSudheendran, Ensuring User Security and Data Integrity in Multi-Cloud, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013 355.
3. Boyang Wang, Baochun Li, Hui Li, Public Auditing for Shared Data with Efficient User Revocation in the Cloud, accepted by INFOCOM 2013, (2013) July15-19;Turin, Italia.
4. AbhinavRaje,BhusawalPant,Assistantprofessor/IT ,International Jour- nal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certi_ed Organization) Vol. 3, Issue 11, November 2015
5. Kan Yang, XiaohuaJia. Data storage auditing service in cloud computing: challenges, methods and opportunities. The journal of World Wide Web. 15, 409(2014)
6. Y. Zhu, H. Hu, G.J. Ahn, M. Yu Menonm IEEE Paper publication 199-1023-2231-2244, 2012-13.
7. Mr. Rajesh H. Davda1, Mr. Noor Mohammed, Text Detection, Removal and Region Filling Using Image In painting, International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 23204486, 2013
8. UdayModha, Preeti Dave, Image In painting-Automatic Detection and Removal of Text From Images, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012.
9. Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, Analysis of Image In painting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods, International Journal of Computer Applications (0975 8887), Volume 9, No.11, 2010
10. Nobuo Ezaki, Marius BulacuLambert ,Schomaker , Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons, Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer
Society, pp. 683-686, vol. II, 2004.
11.A Survey on Recognition-Based Graphical UserAuthentication Algorithms FarnazTowhidiCentrefor Advanced Software Engineering, UniversityTechnology Malaysia Kuala Lumpur, Malaysia
12.Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters, College of IST Drexel University Philadelphia, PA, 19104 USA