Volume 4 || Special Issue 6 || ICCEME 2019-2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

GRAPHICAL SYSTEMS AUTHENTICATION USING ASCII

SAURABH SURYABHAN SANANSE[1], ASST. PROF. V. S. KARWANDE[2]

ME STUDENT,CSE Dept., EVEREST EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS, AURANGABAD[1],
ASST PROF., CSE Dept., EVEREST EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS,AURANGABAD[2],

Abstract- Verification is the procedure by which a user is verified through various kind of security Frameworks, with the end goal to get to their private resources and information in a confidential and protective way. For each security framework on the planet, the main goal is to protect the resources from illegal activity and effectively confirming a legitimate user among different users. In any case, a large portion of the security frameworks are confronting a profound fall in their goals because of various attacks on the system like shoulder surfing attack, dictionary attack, cyber-attacks and so on. As the most popular authentication systems include the utilization of alpha numeric passwords yet they have numerous issues as they are anything but difficult to figure. That's the reason they are not secure to be applicable at all. Graphical passwords contains pictures, logos fill in as a password that are simple for the user to be applicable and have gigantic effect on the mind for quite a while. This proposed work is likewise centered around GUI based authentication system that utilizes intelligent illustration of graphical shapes like square and uses ASCII submission for verification.

Keywords: *Hybrid Authentication; ASCII conversion; Java program; Shoulder surfing; 3D GUI.*

I INTRODUCTION

As the mankind is increasing its steps in the world of technology, a huge blessing from the Mother Nature which means that only the human race is able to achieve the topmost heights of advancement among all species. The rapid increase in technology has made a huge difference between us and other creatures, due to which we make our life very high-yielding in order to sustain compactness and elegance. However, one should remember that there are always some pros and cons behind every advancement. The biggest disadvantage is that humans misuse technology against their own race. In order to sustain this technology and protect them from harm from a security point of view, we have to introduce another level of security which will Govern and control these technical threats and issues related to this. As we start from the computer system that is the basic core of the technology. Many security modules are made to protect these resources, among which the most common security system is based on alpha numeric passwords earlier. There are some critical issues regarding to installing this security in many fields, Not only do these system facing the depression fail, but many security system also face other different types issues such as costly installation, light security, stealing of tokens etc. The main problem in this security technique is the cracking or bypassing these security modules through various type of attacks as the hacker can relate to the user's password through guessing or by standing nearby (shoulder surfing) or by regularly attempting the combination of password (dictionary attack) etc. These problems are common to most security modules. Hence we are proposed GUI based authentication system that utilizes intelligent illustration of graphical shapes like square and uses ASCII submission for verification. Previously used Algorithms The category of graphical authentication are divided into four major techniques:

1.1 Recognition based Technique

In this technique the user has to select the picture, images, logos etc. from the set of images at the registration time, then the user has to identify their picture from the grid of Images for login in the system. Approximately 90% of people easily remember their password after some duration of 1-2 months. Many algorithm based recognition techniques are stated below:

1.1.1. Passfaces: This technique was proposed by Sacha Brostoff and M Angela Sasse in 2000.The aim of this

technique is to provide the major usability feature to the user like ease of access, directly creation and recognition
of password. In this system the user is asked to choose the different face from the set of images of faces from the grid as he/she has chosen earlier at the time of registration.

1.1.2. Dj vu: This technique was proposed by Rachna Dhamija and Drian Perrig in 2000. The main purpose of the system is to ease the process of authentication for the user. Here the user has to select the image from the given set of images. But the main disadvantage of the system is that the system stores the seeds of the image.

1.2. Recall based Technique

This technique stated that the users have to recall their passwords without reminders from the system. It is composed of very easy technique, but users are not quite able to remember their password. Many of the techniques lie in this category:

1.2.1 Syukri: The signature based technique first proposed by Syukri et al in 2005. This technique basically works in two steps: The first step contains
the registration phase in which the user has to draw an initial signature on a touch sensitive screen and the second step contains the verification phase, in which users have to redraw their signature and after some normalization in their drawn signature, the system matches the image with their best case in database for login.

1.2.2 Pass doodle: The technique was proposed by Christopher Varenhorst in 1999. The system algorithm is a GUI based one in which the use of a handwritten drawing or sketch such as doodles are used to make the authentication password. The study said that it is more difficult for the user to crack handmade doodle as they are varying in many ways.

1.3 Hybrid Scheme

The composition of more than one technique is known as hybrid scheme. In this technique, security is formed mainly through the dual mechanism of different techniques built into them. Therefore, its process is very hard and with a complex structure of security, the authentication decision depends on each and every technique used in the system. So it is a bit difficult to challenge the security presented by these systems.

1.4 Cued Recall based Technique

These techniques include hints, gestures and reminders that act as a password key. Due to these easily rememberable things, the users can relate their password and recall them to login in the system. Many of the techniques lie in this category:

1.4.1 Blonder: This technique was proposed by Greg E Blonder in 1996 and was the first ever made after research on authentication through GUI systems. In this technique, the system displays some predetermined images to the user through which user has to point on the images, in order to reach the resource, but in the same sequence at the time of registration.

1.4.2 Passpoint: This technique was proposed by Susan Wiedenback, and others in 2005. The pass point technique can be said to be a new version of Blonder algorithm. The purpose of this technique was to overcome the limitations in the Blonder technique. The algorithm proposes much flexibility in that it requires the user to click in a region not farther than 0.25cm away for an accurate click and therefore the concepts of tolerance is also introduced in their system.

II LITERATURE SURVEY

2.1 Agus Fanar Syukri, Eiji Okamoto, and Masahiro Mambo, “A User Identification System Using Signature Written with Mouse”, Springer, 2006.

A user identification system is very important for protecting information from illegal access. There are identification systems using standard devices (keyboard or mouse) and systems using special devices. In their system, users write a simple figure object and the successful verification rate is 87%. However the simple object is too easy to prevent impersonation. In order to realize a more reliable user identification system using mouse, we propose a new system to identify users using a complex figure object, signature. New techniques we utilize in our system are as follows: the normalization of

input data, the adoption of new signature-writing-parameters, the evaluation of verification data using geometric average means and the dynamical update of database. We have implemented our user identification system and conducted experiments of the implemented system. The successful verification rate in our system is 93%.

2.2 Anne V. D. M. Kayem, "Graphical Passwords - A Discussion", IEEE 30th International Conference on Advanced Information Networking and Applications Workshops, 2016.

Authentications, on web applications and service platforms such as the ones that enable collaborative information sharing and resource management, are typically handled via text based passwords. From a security usability perspective, text based passwords are easy to use and familiar to users. Textbased passwords however, are prone to attacks that stem from challenges that users face with memorability. Text-based password memorability issues pose problems for service providers on platforms where identity management is a key concern. Application examples emerge in social media, online commerce, and also in the management of critical infrastructure such as smart microgrids. A further concern is that, large volumes of sensitive information are made available and shared on these applications and so constitute an attractive target for obtaining data in adversarial ways in order to provoke impersonation and inferential attacks, for instance. In this paper, we discuss the pros and cons of using graphical passwords instead of text-based passwords on information sharing platforms. We support our discussion by considering two graphical password schemes based on the principles of recall and cued-recall respectively which are philosophically similar to text-based passwords. Results from our proof-of-concept implementation indicate that, in comparison to text-based and recall graphical passwords, cued-recall graphical passwords are a better authentication mechanism in terms of memorability and password security.

2.3. Rachna Dhamija, Adrian Perrig, "Dej'a Vu: A User Study Using Images for Authentication", IEEE

Current secure systems suffer because they neglect the importance of human factors in security. We address a fundamental weakness of knowledge based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies on recognition-based, rather than recall-based authentication. We examine the requirements of a recognition-based authentication system and propose Dej'a Vu, which authenticates a user through her ability to recognize previously seen images. Dej'a Vu is more reliable and easier to use than traditional recallbased schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others. We develop a prototype of Dej'a Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90participants succeeded in the authentication tests using Dej'a Vu while only about 70and PINS. Our findings indicate that Dej'a Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords).

2.4. Mrs. Aakansha S. Gokhalea, Prof. Vijaya S.Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique", 7th In-
ternational Conference on Communication, Computing and Virtualization,2016.

Now a days computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization cant occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through various types of attack. So to overcome these vulnerabilities, a graphical password technique is introduced. As name suggests in this technique images (pictures) are used as a password instead of text. Also

psychological study says that human can easily remember images than text. So according to this fact, graphical passwords are easy to remember and difficult to guess. But because of graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. So here, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent. It is a combination of recognition and recall based approach. It can be useful for smart held devices like smart phones, PDA, iPod, iPhone etc.

2.5. Joseph Goldberg and Jennifer Hagman, Vibha Sazawal, "Doodling Our Way to Better Authentication", CHI 2002, April 20-25, 2002, Minneapolis, Minnesota, USA.

Password security often fails in practice because users select predictable passwords. We conducted a study to explore the use of a hand-drawn doodle password ("passdoodle"). Our findings show that users could recall all visual elements of the doodle as well as they could recall alphanumeric passwords, but most could not perfectly redraw their selected doodles. Users perceive passdoodles as easier to remember than alphanumeric passwords; however, they prefer whichever authentication method they perceive to be more secure.

2.6. Wendy Moncur, Grgory Lepltre, "Pictures at the ATM: Exploring the usability of multiple graphical passwords", CHI 2007, April 28May 3, 2007, San Jose, California, USA

Users gain access to cash, confidential information and services at Auto- mated Teller Machines (ATMs) via an authentication process involving a Personal Identification Number (PIN). These users frequently have many different PINs, and fail to remember them without recourse to insecure behaviours. This is not a failing of users. It is a usability failing in the ATM authentication mechanism. This paper describes research executed to evaluate whether users find multiple graphical passwords more memorable than multiple PINs. The research also investigates the success of two memory augmentation strategies in increasing memorability of graphical passwords. The results demonstrate that multiple graphical passwords are substantially more effective than multiple PIN numbers. Memorability is further improved by the use of mnemonics to aid their recall. This study will be of interest to HCI practitioners and information security researchers exploring approaches to usable security.

III SYSTEM ARCHITECTURE

Proposed system works on the hybrid approach of authentication system that uses both textual and graphical security modules. Textual password comprises of a small portion of alphanumeric security in order to check whether the user is authentic or not, for registration or for login. If the authenticity proves in the users favour, and the user is then forwarded to the next part i.e. graphical password. In graphical password where he /she is able to mark different squares on the given 3D matrix as a password. By marking each square with a mouse, the ASCII value is generated corresponding to the values displayed on the 3D matrix on the server side.

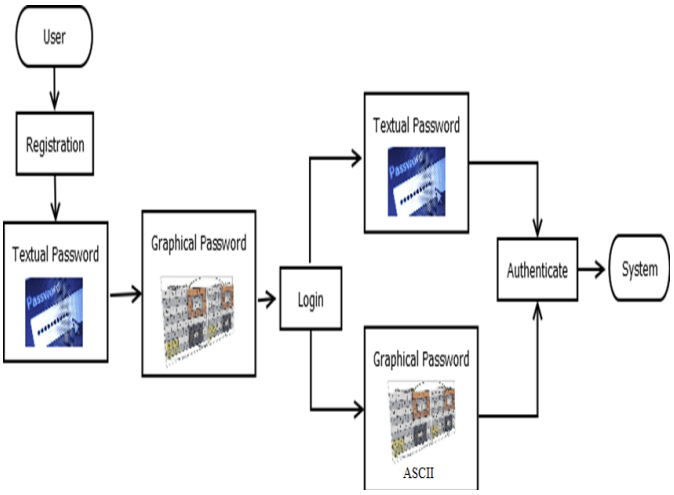

Fig 1: System Architectural

3.1 Activity Diagram

Activity diagram can be defined as a flowchart to display the flow from one activity to another activity. These activities could be described as an operation of the system. The control flow usually is drawn from one operation of application to another. This can be branched or sequential, or concurrent also. Activity diagrams can

deal with all or many type of flow control and used different elements such as join or fork.

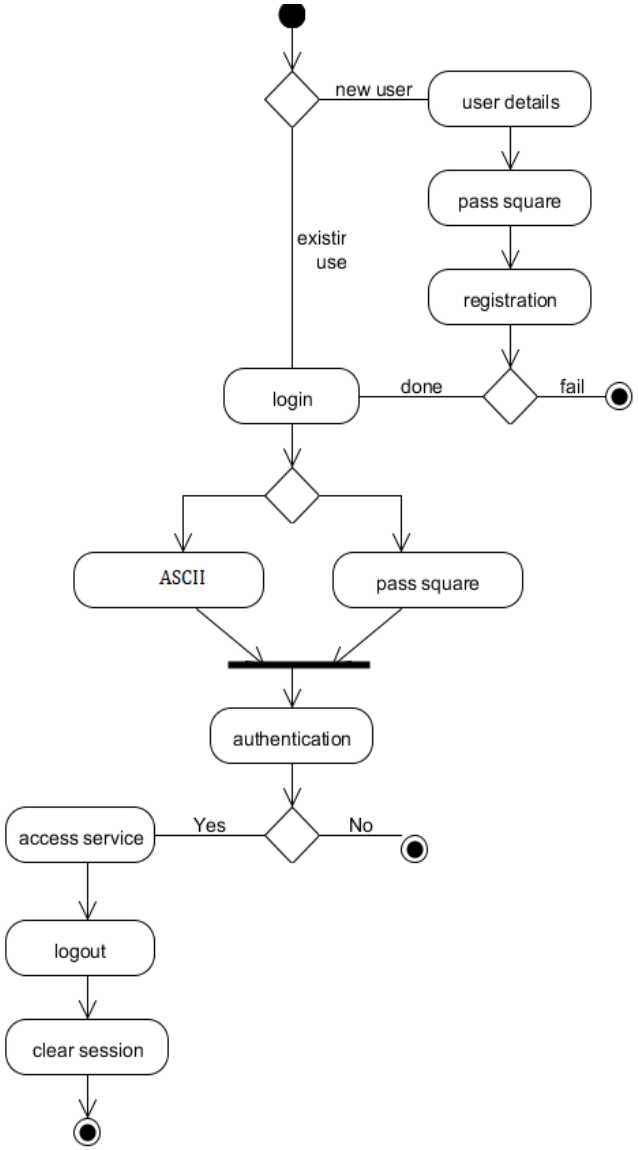

Fig 2: Activity Diagram

IV RESULT

4.1 Module 1: Registration

As the system is hybrid, the registration phase contains two parts of authentication technique.

4.1.1. Textual based password

In this part, the users have to register their textual based identity with the system. Therefore it is necessary for users to fill their required credentials. After being registered in the textual password, the system processes the user on graphical phase.

4.1.2. Graphical Password

In this security module, the user has to mark the different combination of squares in order to make graphical password and press save button after selecting each combination on 8x8 matrix. Here the total number of possible different combination of square formed in the system are shown in Table I. We exclude 1x1 square combination in our system, so the total number of combination of square are formed=140.

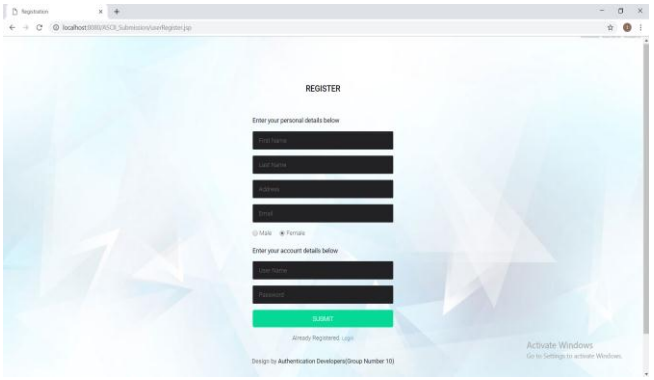

Fig 3: Registration Page

4.2 Module 2: Login

4.2.1. Working of login phase

In order to login into the system, the users need to enter their username and password in the text based security module, if the given information successfully matches with registered information, then the system processes the user to graphical security module where the user simply has to mark the same combination of squares as he/she has marked at the time of registration.

4. 2.2. Explanation of login interface

A login form is displayed with some information for better understanding. Here, the form contains the columns for the Username and the Password in which the user fills the details in the given column. Username: & Password. After giving the details, the information is checked in parallel through the authentication phase. If the given textual based information matches, then the users proceed to the graphical part of the system in which they have to mark their different combination of squares same as marked in registration phase. Therefore

after selecting the combination of squares, their login single set values are formed same as in registration phase.

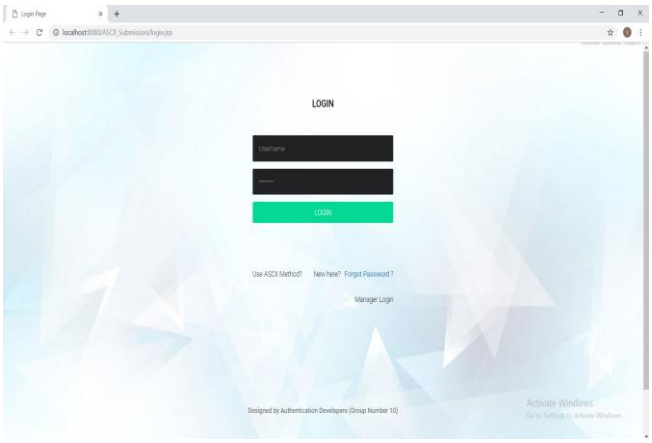

Fig 4: Login Page

4.3 Module 3: Authentication

Coming on the verification process, the information that is given in login phase are matched simultaneously with the information at registration time. If the given information is correct, the system will forward the user to the graphical module at login time. We now come to the graphical module. After marking the combination of square on 8x8 grids and the system generates the single set of values, these single set of values are compared to the values of login time and registration time, for correct matching. If the login set values and registration set values are matched correctly then the system will successfully authenticate the user.

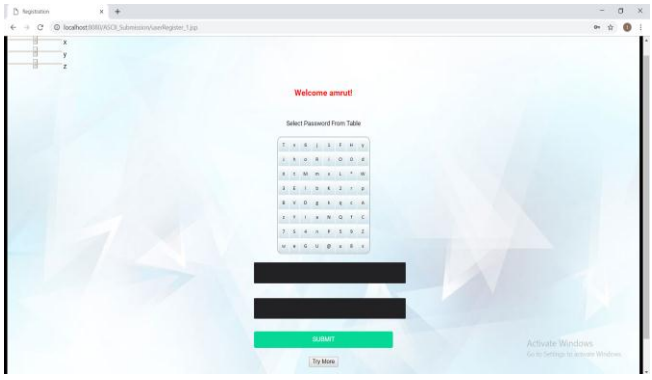

Fig 5: Password Table

V CONCLUSION

In this Paper, we have proposed a model that for each security framework on the planet, the main goal is to protect the resources from illegal activity and effectively confirming a legitimate user among different users. Our proposed system is to give a robust security which will protect our resources and information from the illegal activities and make the digital era in the world more secure. Our system is focused GUI based authentication system that utilizes intelligent illustration of graphical shapes like square and uses ASCII submission for verification. Our aim is to give a robust security system which will protect our resources and information from the illegal activities and make the digital era in the world more secure. Now times I am working on the security system which is specially designed for the blinds, which validate the user through biological receptors. Through this system any blind person can easily authenticate in same mean time as the normal person, not only the blind any normal person can use this system. The other security system is based on cybernetics which is also the duplex combination of biometric and graphical modules that uses DNA detection, biological imprints for authentication. We are very much inspired from the view of Digital India as well as studies conducted on medieval people that shows transformation of people through different level of education.

REFERENCES

[1] Agus Fanar Syukri, Eiji Okamoto, and Masahiro Mambo, “A User Identification System Using Signature Written with Mouse”, Springer, 2006.

[2] Anne V. D. M. Kayem, “Graphical Passwords - A Discussion”, IEEE 30th International Conference on Advanced Information Networking and Applications Workshops, 2016.

[3] Rachna Dhamija, Adrian Perrig, “Dej‘a Vu: A User Study Using Images for Authentication”, IEEE.

[4] Mrs. Aakansha S. Gokhalea, Prof. Vijaya S. Waghmareb, “The Shoulder Surfing Resistant Graphical Password Authentication Technique”, 7th International

Conference on Communication, Computing and Virtualization, 2016.

[5] Joseph Goldberg and Jennifer Hagman, Vibha Sazawal, "Doodling Our Way to Better Authentication", CHI 2002, April 20-25, 2002, Minneapolis, Minnesota, USA.

[6] Wendy Moncur, Grgory Lepltre, "Pictures at the ATM: Exploring the usability of multiple graphical passwords", CHI 2007, April 28May 3, 2007, San Jose, California, USA.

[7] Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo and Hongxin Hu, "On the Security of Picture Gesture Authentication", 22nd USENIX Security Symposium, 2013.

[8] ASN Chakravarthy, P. S. Avadhani, S. N Krishna Prasad, N. Rajeev and D. Rajasekhar reddy, "A Novel Approach For Authenticating Textual Or Graphical Passwords Using Hopfield Neural Network", Advanced Computing: An International Journal (ACIJ), July 2011.

[9] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences Journal, 2012.

[10] Dr. M. Newlin Rajkumar, V. Dhurka and P. Kayathri, Survey a Secured Privacy Authentication with Recovery", World Scientific News, 2016.

[11] Yean Li Ho, Bachir Bendrissou, Afizan Azman and Siong Hoe Lau, "Blind- Login: A Graphical Authentication System with Support for Blind and Visually Impaired Users on Smartphones", American Journal of Applied Sciences,2017.