ZKG INTERNATIONAL

ISSN: 2366-1313

WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

[1]Mrs. M. Srimathi, [2]Sandhyala Sai Kiran, [3]Gijja Sai Prasad, [4]Arella Nikhil

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

srimathi.marella@gmail.com

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

sandhyalasaikiran@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

gijjasaiprasad@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

nikhilarella2002@gmail.com

Abstract: *User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. However, it has its disadvantages like easy or short passwords are easy target of dictionary and brute-forced attacks and Difficult passwords are hard to remember. Hence, we propose to use graphical passwords, in which graphics (2D images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches. The operation of the purposed scheme is simple and easy to learn for user since they familiar with textual graphical password scheme. In conclusion, this graphical password scheme will make it easier for user to do their authentication process since it is easy to remember and hard to guess by other.*

Keywords: *Authentication, Graphical Passwords, Image Slicing, Encryption*

I. INTRODUCTION

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most of the authentication system nowadays uses an integration of username and password. The problem with the password is that it requires user to remember it and it should be kept secret. Each authentication system has its own

ISSN: 2366-1313

guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate number, parent name, phone number sometimes their own name which are very much predictable or complex passwords which they overlook so they might be use the same password for different accounts or they jot down their password somewhere. Moreover, user is vulnerable to various attacks. Text-based passwords faces from security and usability matters[1].

To overcome these shortcomings of alphanumeric passwords, graphical password schemes have been proposed. In graphical password authentication application by using passpoints scheme a password contains an image where user can input password with the help of mouse events like click and drag. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by human brain, enhancing the ability to. Strong passwords can be invented which are resistant to guessing, dictionary attack and social engineering.

In the literature, several techniques have been proposed to reduce the limitations of alphanumerical password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word [2]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches

GRAPHICAL PASSWORD

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words [8]. Also, they should be more resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques [3]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Passfaces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces. An early recall-based

ISSN: 2366-1313

graphical password approach was introduced by Greg Blonder in 1996. In this approach, a user creates a password by clicking on several locations on an image. During authentication, the user must click on those locations. PassPoints builds on Blonders idea, and overcomes some of the limitations of his scheme. Several other approaches have been surveyed in the following paper.

II. LITERATURE SURVEY

This chapter discussed about the related research that is review for Graphical Password Authentication which are being proposed. Generally, this including a few articles and journal that related directly and indirectly to the secure graphical password system. All this research was described, summarized, evaluated and clarified. It is a regulation in order to establish the credibility for a better project

PassPoint Method

In this paper it is an extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. The image could be any natural picture or painting then it contains several possible clicks points. As a result, a user can click on any place on an image (as opposed to some pre- dined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence as in Figure 1. When using this method user might easily able to quickly create a valid password[4].

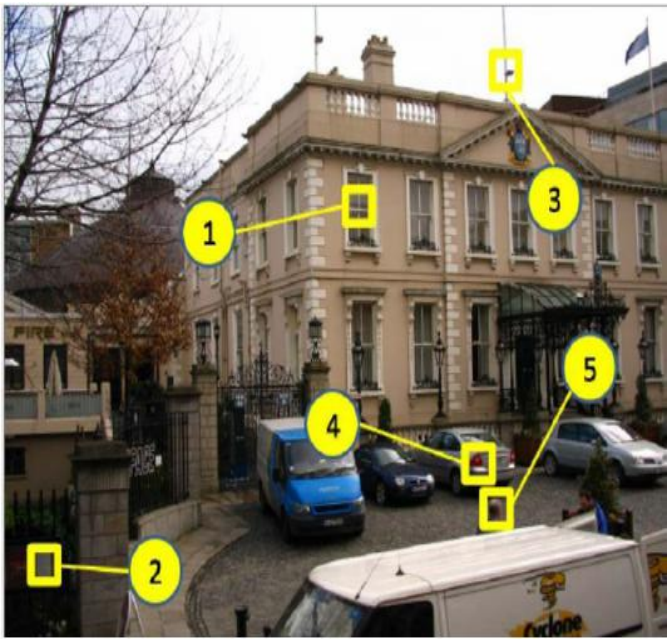

Fig.1 A Sample of PassPoint Method

Blonder Graphical Password Scheme

Single-image based schemes use one single image as a background, and require a user to repeat several actions with an input device, such as clicking or dragging in the same manner as in the registration stage

Blonder gave the initial idea of graphical password. In his scheme, a user is presented with one predetermined image on a visual display and required to select one or more predetermined positions on

ISSN: 2366-1313

the displayed image in a particular order to access the restricted resource. The major drawback of this scheme is that user cannot click arbitrarily on the background. The memorable password space was not studied by the author either.

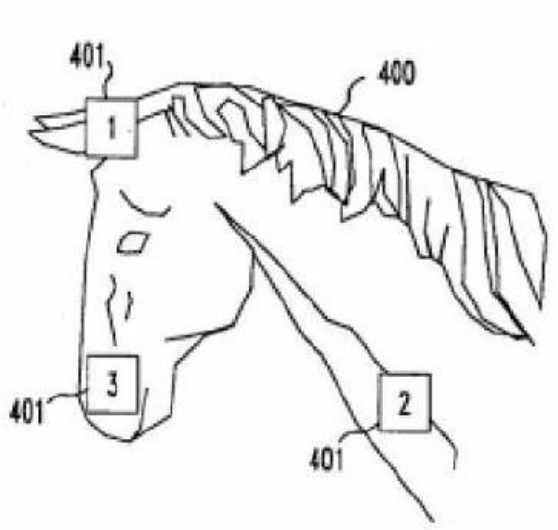

Fig.2 Graphical password scheme suggested by Blonder

Security in Graphical Password Authentication

According to the paper, the first defence for computer system is authentication. Graphical authentication may offer greater resistance to guessing and capture attacks but there are other attacks against graphical authentication including social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware which those attacks might be threats to the security breach. Authentication mechanism that often being used is the combination of usernames and passwords which is based on textual-based password. Nevertheless, this traditional approach had shown some disadvantages. The significant consequences of the approach are the user might choose simple password for authentication process or the user can create a strong password however it is hard to be remembered by the user itself. This paper mentioned about three categories of the graphical authentication scheme which are Draw metric schemes, Search metric schemes and Locimetric system. There are also CAPTCHA, but it is not based on recognition or re-creation password like the other graphical password but it is relied on human (as opposed to computer) abilities to recognize obfuscated text displayed in form of image. There is also hybrid scheme which is made up of combination of two or more schemes. By using graphical password scheme, it can provide highly secure authentication process by enable the user to remember the complex password easily. And it also can be used as defence to the shoulder surfing, Spybot and similar compromises of user systems. The highly secure authentication system can be achieved by adding some security features in graphical user authentication[5].

ISSN: 2366-1313

Multiple-image schemes

In multiple-image schemes, on the other hand, multiple images are presented and a user is required to recognize and identify one or more of it, which are previously seen and selected by the user. Psychological studies suggest that people are much better at imprecise recall, particularly in recognition of previously experienced stimuli. This class of passwords was shown to be remembered by user for a long period after short perception

Wantong Zheng and Chunfu Jia proposed a method "Combined PWD". This scheme proposes an online secret phrase verification component, combined PWD, through embedding separators (e.g., spaces) into the passwords to reinforce the current secret word validation framework. This plan uses the custom of the client's input. In this examination, site clients can embed spaces in their secret word where they need to stop when they register a record and the site back-end records the number of spaces in each hole [6].

In the paper [7] , a novel time-based unique password was contributed to avoiding challenges of using a third party such as one- time password email, test and token device, the client will set an underlying secret word to characterize how the secret key will be changing throughout a characterized time, we tracked down that the framework. Then found that the system retains the strength of the dynamic password and improves the usability of the system in terms of availability.

A strong password authentication scheme was proposed by Yang Jingbooo. The one-time password authentication schemes can be divided into two types namely weak password authentication schemes and strong-password authentication schemes. In this paper, we survey the as of W.C Ku‟s scheme and it also shows an attack against his protocol. And also found that strong passwords have higher strength and easily guessing is not possible. Later, we present a strong password authentication scheme. This paper expands W. C. Ku's plan so that the alteration convention can oppose Stolen-verifier assault. The changed convention is built without loss of effectiveness[8].

Hua Wang, Yao Guo proposes another reuse- situated secret phase authentication system, called Desktop Password Authentication Center (DPAC), to reuse counter-measures among applications, along these lines lessening the expense of protecting passwords against dangers. This arrangement can take out a ton of tedious work and reduces the expense essentially, we demonstrate the feasibility ofDPAC by

ISSN: 2366-1313

implementing a prototype, in which we migrate the widely used OpenSSH to DPAC and implement two example countermeasures [9] .

Password authentication code (PAC) is a very important issue in many applications such as web- sites and database systems etc. Salah Refish proposes a PAC-RMPN scheme. In this paper, PAC between two clients to affirm verification between them has been introduced. This research presents a novel solution to the era-long problem of password authentication at the incoming level. They should discover a strategy to secure this a secret word from anticipated attackers. A legitimate user types his password only and presses enter topropagate it to another user which he wants to be authenticated [10] .

A secure password authentication scheme is proposed which gives more security. This method uses a combination of pattern, key, and dummy digits.For this, the client needs to perceive and enlist design asarea numbers from the network, register key qualities that guide esteem to secret password, and attach fakerqualities to misguide the attacker. From that point forward to log in, the client needs to review the example and guides the secret key from design with enrolled key qualities, making a secret word by including sham digits. It minimizes shoulder surfing, brute-force attacks, cross site scripting etc. due to the high complexity of guessing passwords in multi-levels:first from the pattern, then from key, and then fromdummy values [11].

III. PROPOSED WORK

The proposed authentication system works as follows. At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

For authentication, the user first enters his or her username. The system, then, displays the registered picture. The user, then, has to correctly pick the POIs and type the associated words. At any time, typed words are either shown as asterisks (*) or hidden.

The proposed authentication system works as follows. At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest

ISSN: 2366-1313

(POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

SYSTEM ARCHITECTURE:

System Architecture is a sketch of following process that allows how the system works and happen. Figure 4.1 shows that user can register to the system by enter username, email and phone number and then user is required to select a picture displayed. At this point, user need to click any five points in the picture that had been chosen before. After that, registration information will be saves in database. During login phase, user need to insert the username that has been registered during registration phase. Then, user is required to verify the picture displayed in the application that they had choose during 18 registration phases. After that, user is required to click five points that they clicked during the registration phase respectively. The system will make a comparison by checking the information with database. The database server will send result whether user have registered or not to the user. Finally, user will be authenticated if the information entered and given by user are all correct.

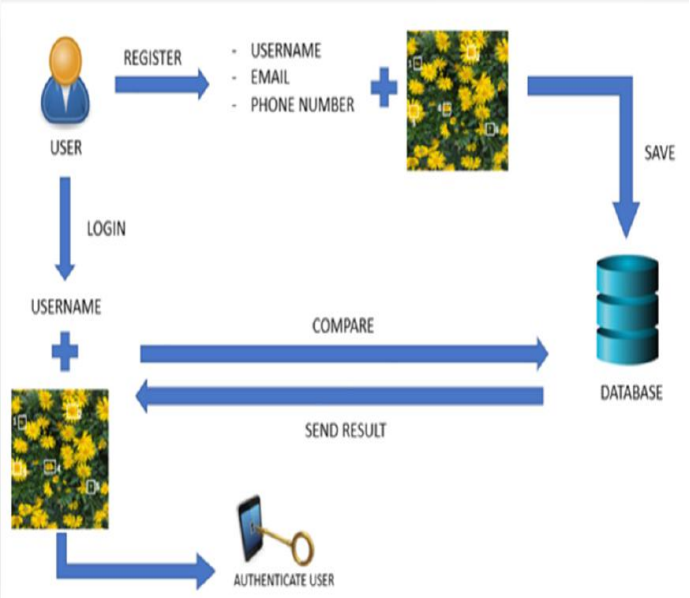

Fig.3 System architecture.

IV. RESULTS

ISSN: 2366-1313

Fig.4 Home page

Fig.5 New user registration page

ISSN: 2366-1313

Fig.6 password image page

Fig.7 Mouse location spots entered

Fig.8 user login page

Fig.9 user authentication page with choosing spots

ISSN: 2366-1313

Fig.10 click points as a password

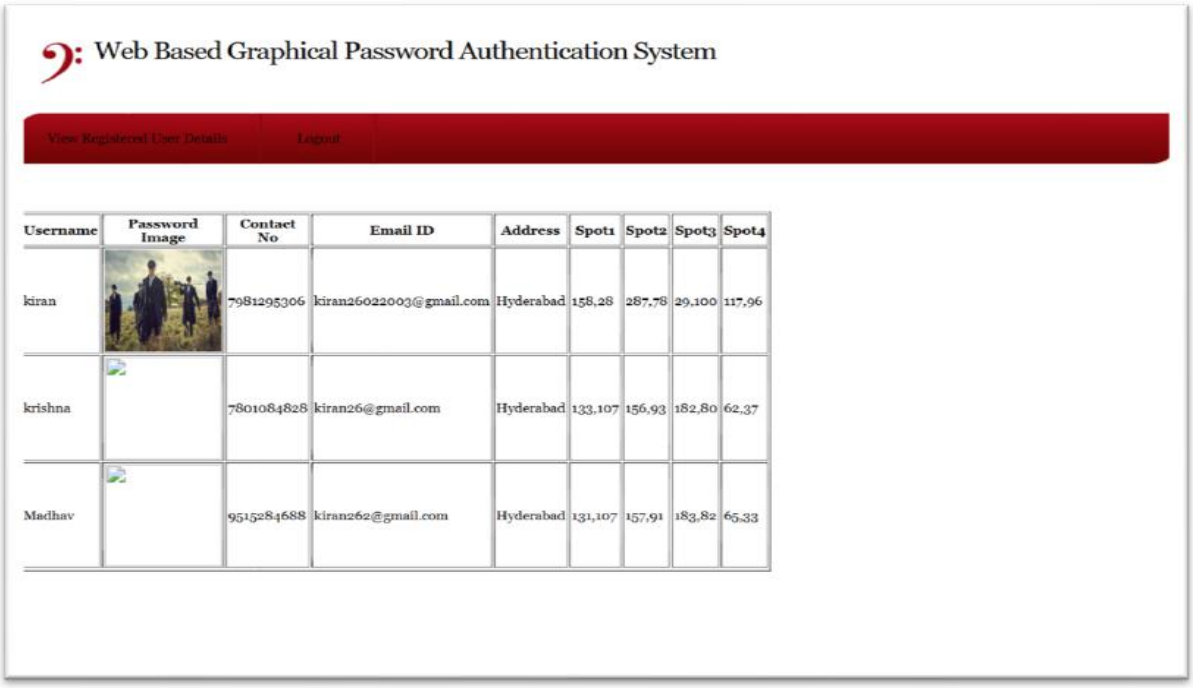

Fig.11 Admin home page

V. CONCLUSION

In conclusion, This Graphical Password Authentication System provides a secure and user-friendly alternative to traditional text-based passwords. The system's use of personalized passpoints, which are selected and arranged by the user, makes it difficult for attackers to guess or brute force the password. Additionally, the system's use of graphical elements adds an

ISSN: 2366-1313

extra layer of security, as it is difficult for attackers to recreate a user's selected passpoints without access to the original image. Overall, the Passpoints system has proven to be a effective and secure method of authentication, making it a valuable tool for protecting sensitive information and assets. The Passpoints system also offers the added benefit of being easy for users to remember, as the passpoints are chosen by the user and are based on personal information or interests. In addition, the system is flexible and can be easily integrated into a variety of different systems and applications.

REFERENCES

1. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. p. 26.

2. Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.

3. Ahmet Emir Dirik, Nasir Memon, & Jean-Camille Birget. (2007). Modeling user choice in the PassPoints graphical password scheme. 8.

4. Nelson, D. L., Reed, V. S., & Walling, J. R. (1976). Pictorial superiority effect. Journal of experimental psychology. Human learning and memory, 2(5), 523–528.

5. Dhamija, R. (n.d.). Hash Visualization in User Authentication. 2.

6. Khan, W. Z., & Aalsalem, M. Y. (19 December, 2013). A Graphical Password Based System for Small Mobile Devices. p. 11.

7. Manjunath G, Satheesh K, Saranyadevi C, & Nithya M. (2014). Text-Based Shoulder Surfing Resistant Graphical Password Scheme. 4.

8. N.Asokan. (16 May, 2014). A Closer Look at Recognition-based Graphical Passwords. p.

9. Tao, H. (2006). Pass-Go, a New Graphical Password Scheme. 11.

10. Towseef Akram, Vakeel Ahmad, Israrul Haq, & Monisa Nazir. (2017). Graphical Password Authentication. 7.

11. Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, & Pranjal Rathod. (2013). Secure Authentication with 3D Password. 7.

12. Zheng, Z., Xiyu Liu , Lizi Yin , & Zhaocheng Liu. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. 8.