JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

COMPARISON TECHNIQUES OF GRAPHICAL PASSWORD

Ms. Hetal Rahul Modi [1], Research Scholar , School Of Pure & Applied Sciences , Department Of Computer Applications ,Sabarmati University , Ahmedabad

Dr. Nayan Soni [2] , Assistant Professor. , School Of Pure & Applied Sciences , Department Of Computer Applications , Sabarmati University , Ahmedabad

ABSTRACT :

Authentication of users is a crucial aspect of security. There are numerous authentication systems in use, including alphanumeric usernames and passwords. However, because of the method's well-known flaws, graphics-based passwords were suggested as a replacement. Graphical passwords are an alternative to alphanumeric passwords because remembering alphanumeric passwords is a difficult task. When a user-friendly authentication system is available for a certain application, it becomes much easier to access and utilize that Application. According to psychological studies, the human mind can readily retain visuals rather than alphabets or figures, which is one of the main justifications behind this strategy. This paper discusses graphical password techniques, which are divided into four categories: recognition-based, pure recall-based, cued-recall-based, and hybrid-based techniques.

Keywords*: Graphical password, Recall-based, Recognition Based*

INTRODUCTION:

In the modern computerized world, where personal information is transmitted by wire, on various carriers, or simply by the air, many users have questions about the safe transmission of their information [3]. Graphical passwords are an alternative to alphanumeric passwords in which users verify themselves by clicking on graphics rather than inputting alphanumeric characters. Graphical passwords are simpler to remember than alphanumeric passwords because an image of a flower is easier to recall than a series of alphabets and numbers. In comparison to verbal or text-based information, human brains appear to have stronger memory for recognizing and recalling visual information such as images, according to several psychological studies. Text cognitively represented symbols that provide meaning that is related with the text, as opposed to meaning that is perceived based on the alphabet's form. Because the size of the alphanumeric corpus is restricted, using images instead of characters will assist the user improve security. But in the case of graphical password, the size of the corpus is infinity if it is in the case multiple numbers of images or if it is in the case of multiple points in single image [20]. The most crucial aspect of real-time security is customer security, which is the bank's primary priority. In order to protect user accounts, authentication must be secure. Textual passwords are the most commonly used method. The method uses a graphical password to illustrate the security of the banking website, offering a possible alternative to traditional alphanumeric password techniques. Because there are numerous security breaches that can occur during a financial transaction, the system uses a two-step verification method to secure the transaction [17]. Knowledge-based systems, token-based systems, and biometrics-based systems are the three basic types of authentication techniques [1].

WHY GRAPHICAL PASSWORDS?

Alphanumeric passwords are commonly used to gain access to computer systems. Users, on the other hand, have a hard time remembering long and random-looking passwords. Instead, they design passwords that are short, basic, and insecure. Graphical passwords were created in order to make passwords more memorable and easier to use, as well as more safe. Users click on graphics rather of typing alphanumeric characters while using a graphical password [14].

ARCHITECTURAL DESIGN:

The system secures the user's transactions using the session password mechanism, which is secured in the first phase using the pass-point technique. The user's click points in the photos created during the registration process are utilized to validate the authenticated user in this technique. The utilization of color palettes is used in the second step of the verification. Instead of the traditional number pad, each number is represented by a pair of colors. After that, the authenticated user is free to continue with the transaction. When a user fails to enter a valid password three times, he or she is flagged as a misuse and a complaint is made against them via the Electronic Filing system. In the event of an unusually large transaction, the user is notified and sent a one-time password [17].

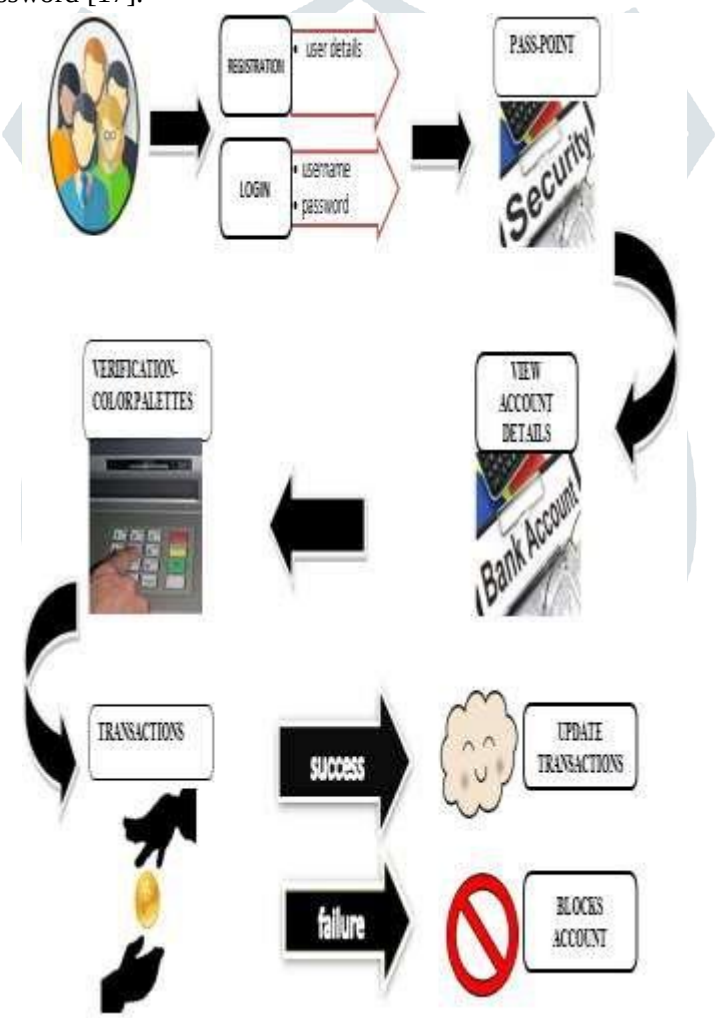

Figure 1.1: Architecture Diagram [17]

PASSWORD TECHNIQUES: We have below mention explain various types of passwords techniques.

Textual or Alphanumeric Password: Text/Alphanumeric (it can also be called a text-based password) is a combination of characters or words used to verify authorized users. This user authentication technique has been in common use for a long time because this technique has many advantages, but before that it was more likely to be stolen by hackers. To reduce the risk of password theft, passwords should be at least eight characters long with uppercase, lowercase, special, and alphanumeric characters. An alphanumeric password should not have anything meaningful like your last or middle name, age, date of birth, school name, etc [5].

Smart Card Authentication: This technique is also used for user authentication and this type of authentication also provides enhanced security. One of the main advantages of smart card authentication is that it can be easily combined with

other types of authentication systems. Smart card authentication provides additional security and protection protocols. Smart cards have a small chip. All user information is stored in the chip of the smart card. Users swipe their smart card into the smart card reader to verify identity [5].

Biometric Authentication: Biometric authentication is a technique that uses an individual's physical characteristics. In this technique, biological data or body factors are evaluated to verify the identity of the user. Biometric authentication provides the strongest security, most foolproof, and system protection against unauthorized users compared to text, graphic, or smart card authentication. There is no chance for hackers to steal biometric based passwords [5].

Graphical Password: The idea of graphical password was introduced by Blonder in 1996, which states that an image must appear on a certain screen and that the user must select certain regions by clicking on the image, if the selected areas of the image are correct, the user will be authenticated. Graphical user authentication is very popular nowadays. Organizations or companies are trying to adopt this authentication technique. On the web, images are also used as a reCAPTCHA to know the type of user. Images in reCAPTCHA form provide enhanced security [5].

GRAPHICAL PASSWORD AUTHENTICATION: In graphical password authentication images are used by the user for authentication, user select some specific regions, select multiple images or create image etc [5].

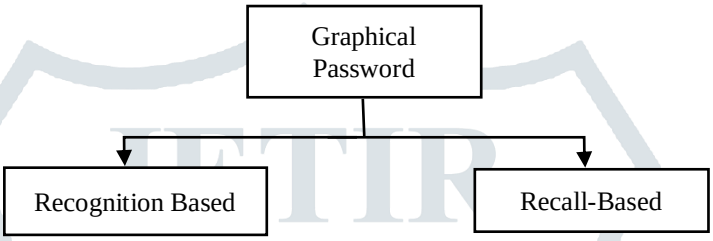

Figure 1.2: Categorization of Graphical password authentication techniques

Mainly graphical password authentication based on two different techniques [5]:

- Recognition Based Technique: In this type of graphical authentication technique, multiple images are shown to the user during the recording phase, the images may be in random order. User must select image (under defined condition) to choose password. The image is selected for the password in sequence or in random order. When logging in, the user has to choose the selected pictures as the password (sequential or random) [5].
- Recall Based Technique: In this technique the user has to provide certain information at the time of recording i.e. handwritten text or drawings. Usually, it is compatible with touch screen devices, pattern selection, signatures, images drawn on 2G grids, password tricks, and more. Techniques of secrecy and signatures. (2) Techniques based on indexed recall include PassPoints, Blonder, VisKey SFR, PassGo, Drawing Geometry and Passlogix VGo techniques [5].

COMPARISON OF METHODS:

Techniques	Description
Recall-Based Technique	This category is very simple and convenient, but it seems that users hardly remember their passwords. However, it is more secure than the knowledge-based technique [20].In these techniques, the user is prompted to reproduce (recall) something that he created or selected earlier in the recording step [20].
Cued Recall-Based	In this category, the user receives a reminder or tip. Prompts help users to regenerate their password or help users to regenerate a more accurate password. This is similar to revocation-based schemes, but it is a registered callback [12] [20].In these techniques, the user is prompted to recall previously saved passwords. Benchmarks provide more clues for users to remember passwords and are therefore easier than techniques based solely on revocation [19].
Hybrid Schemes	In this category, authentication will generally be a combination of two or more schemes. These schemes are used to overcome the limitations of a scheme, such as spyware, shoulder surfing [12] [20].
Recognition Based	Recognition-based systems are also known as cognometric systems. These systems often require the user to remember the category of images during password generation, and upon login, the user must recognize the fake images. The exceptional human ability to recognize previously seen images has made recognition-based algorithms more popular. Various recognition-based systems have suggested using different types of images, mainly faces, icons,

	everyday objects, random art, etc [20]. In this case, to register, the user has to choose some pictures from a random set of images as a password, and for authentication, the user has to identify (identify) these images one by one. sequentially [19].
Pure Recall Based	A Pure recall-based graphical password system is also known as a drawing metric system because the user remembers the sketch on the grid that they created or selected during the save phase. In these types of systems, users often draw their passwords on a grid or blank canvas. Memorization is difficult in which case revocation is difficult because the rollback is done without any index or index [4].

SECURITY ATTACKS ON GRAPHICAL PASSWORD SYSTEMS:

Attacks	**Description**
Dictionary Attack	In this type of attack, the attacker tries to guess the password from a dictionary which is a collection of word lists. The dictionary includes all passwords based on previous selections and all passwords are high probability. So, if the user chooses a password from the dictionary, the attack is successful. This attack is based on password brute force [12][19].
Guessing Attack	Usually, users prefer to choose a password based on their personal information like home name, phone number, etc. In most of these cases, the attacker tries to guess the password by accessing the user's private information. Password guessing attacks can be classified into two categories: online password guessing attacks and offline password guessing attacks. In online password guessing, the attack guesses the password by manipulating input from one or more spells. In offline mode, a password-guessing attacker searches for passwords by manipulating the entries of one or more oracles [12].
Shoulder Surfing Attack	In a shoulder surfing attack, the attacker monitors the user's behavior based on direct observation techniques. One of the techniques of direct observation is to look over the person's shoulder for a password. It usually occurs in public places [12][19].
Spyware Attack	Spyware is a type of malicious software that is installed on a user's computer for the purpose of stealing information about the user. The method to carry out a spyware attack is to use a keylogger or key listener. This malware collects information about users without their knowledge and thus discloses this information to strangers [12].
Social Engineering Attack	A social engineering attack takes place through human interaction to trick users into providing sensitive information. In this type of attack, an attacker disguises himself as an employee of an organization and tries to interact with the user to gather information related to the organization. The attacker does not use any kind of electronic device but with his intelligence and delicate way of conversing to get the information he wants [12].

CONCLUSION:

In this paper "COMPARISON TECHNIQUES OF GRAPHICAL PASSWORD", would ease a new way of securing, processing and retrieving the users data. Analysis found number of method and techniques with efficient and Robust Approach. Thus conclude hybrid approach provide better security and Privacy with different attacks and gives a linear variation as compared to other methods.

REFERENCES:

[1] Jaffar Abduljalil Jaffar, Ahmed M. Zeki, "Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability", IEEE, 2020.

[2] Jiya Gloria Kaka, Ishaq Oyefolahan O, Ojeniyi Joseph O., "Recognition-Based Graphical Password Algorithms: A Survey", IEEE, 2020.

[3] Altaf Khan, Dr. Alexander G. Chefranov, "A Captcha-Based Graphical Password With Strong Password Space and Usability Study", IEEE, 2020.

[4] Abhilash M Joshi, Balachandra Muniyal, "Authentication Using Text and Graphical Password", IEEE, 2018.

[5] Nikita Zujevs, Authentication by Graphical Passwords Method 'Hope', IEEE, 2019.

[6] Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir, "Text based Graphical Password System to Obscure Shoulder Surfing", IEEE, 2018.

[7] Noor Ashitah Abu Othman, Muhammad Akmal Abdul Rahman, Anis Shobirin Abdullah Sani, Fakariah Hani Mohd Ali, "Directional Based Graphical Authentication Method with Shoulder Surfing Resistant", IEEE, 2018.

[8] Bilal Eid Fayyadh, Khalid Mansour, Khaled W. Mahmoud, "A New Password Authentication Mechanism Using 2D Shapes", IEEE, 2018.

[9] Gi-Chul Yang, "PassPositions: A Secure and User-Friendly Graphical Password Scheme", IEEE, 2017.

[10] Jina Marin Bijoy, Kavitha.V.K, Radhakrishnan.B, Dr.L.Padma Suresh, "A Graphical Password Authentication for Analyzing Legitimate User in Online Social Network and Secure Social Image Repository with Metadata", IEEE, 2017.

[11] B. Aravindh, V.D. Ambeth Kumar, G. Harish and V. Siddartth, "A Novel Graphical Authentication System for Secure Banking Systems", IEEE, 2017.

[12] Rebeiro Caroline Leontia Carlton Christopher, Huda Noordean, "A Survey on Graphical Password Authentication System and their Security Issues", IJIRSET, Vol. 6, Issue 6, June, 2017.

[13] Shiksha Saxena, Nikesh Tiwari, "A survey on Graphical Password Authentication", IJERT, ISSN: 2278-0181, Vol. 4 Issue 12, December-2015.

[14] Miss. Saraswati B. Sahu , Associate Prof. Angad Singh*, "Survey on Various Techniques of User Authentication and Graphical Password", IJCTT, ISSN: 2231-2803, Volume 16 number 3 – Oct 2014.

[15] Muhammad Ahsan, Yugang Li, "Graphical Password Authentication using Images Sequence", IRJET, 2017.

[16] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "Graphical Password Authentication", IEEE, 2014.

[17] Heera K*, Anusuya M, Kaviyaa V, Lavanya AK4, Shanthi R, "Graphical Password Authentication for Banking System", IRJET, 2020.

[18] Ragavendra .A, Jeysree .J, "Graphical Password Authentication Using Carp", IJARCET, 2015.

[19] Aakansha Gokhale, Vijaya Waghmare, "Graphical Password Authentication Techniques: A Review", IJSR, 2013.

[20] Dhanashree Kadu, Dhanashree Kadu, Anil Chaturvedi, "Different Graphical Password Authentication Techniques", ICEMTE, 2017.