Full Paper

A SURVEY ON GRAPHICAL BASED AUTHENTICATION MODEL FOR SECURE ELECTRONIC PAYMENT

Sani Suleman Isah Atsu
Federal University of Technology,
Minna, Nigeria
sani.pg918915@st.futminna.edu.ng

John Kolo Alhassan
Federal University of Technology,
Minna, Nigeria
jkalhassan@futminna.edu.ng

Mohammed Danlami Abdulmalik
Federal University of Technology,
Minna, Nigeria.
drmalik@futminna.edu.ng

ABSTRACT

Client authentication is an essential component in nearly all electronic payment systems. This provides foundation for client the legal access control and user liability. The most foremost used authentication technique is the textual or traditional alphanumeric password. However, this method suffers several setbacks. For instance, clients usually choose passwords that can be easily guessed, thus, compromising security of the user's password information. Furthermore, when the password is tough to predict, it will all also be tough to remember. To resolve these challenges highlighted in this context, graphical authentication methods are proposed. Many authentication-based applications including electronic payment systems find the use of graphical password to be robust especially with regards to security and ease of use. Hence, in this research work, a thorough comprehensive analysis is carried out on existing graphical authentication password techniques with keen emphases on their suitability for electronic payment systems. This survey has shown that graphical based password technique would be the most reliable authentication technique for e-payment systems.

Index Terms:
User Authentication, algorithm, recall based, recognition based, Graphical Passwords, knowledge authentication password mechanisms, shoulder surfing attack,

1. INTRODUCTION

The most globally technique in knowledge-based authentication method is username and textual based passwords otherwise known as the alphanumeric password. While working at the Massachusetts Institute of Technology, Fernando Corbato, was the first to introduce the idea of computer password [1, 2]. The traditional method of authentications has found application in several domains that include the electronic payment systems. For example, difficulties in remembering passwords are major disadvantages. Research works have revealed that users have a habit of picking non-lengthy passwords or passwords which are simple to recollect such as nickname, given or a combination of names. And so, these passwords suffer drawbacks and it is easily predicted or hacked. [1, 2, 3, 4] in their research work, stated that "in a computer world, a team of security at a big company tested through a network password cracker by investigation and unexpectedly in a period of half a minutes, succeeded in cracking eighty percent (80%) of the passwords". Furthermore, passwords which are difficult to predict or breakdown by attackers are often not ease to remember. And so, huge area of the client services calls is similar or getting their password. Past research works indicated those memories of human beings only remember shortcomings of textual or alphanumeric passwords. This is as a result of the restriction that they may write down their password in an unencrypted form and are found of using unique or particular one single password for other applications [4].

[5, 6] introduces graphical passwords as another means of user authentication that uses image as password instead of numbers and text (alphanumeric). Here an image is presented on visual screen where the user will click upon a few selected areas of the image. If the right area or regions are clicked in, then the user will be authenticated. The idea is geared up by ability to remember picture images perfectly compared to textual characters and to further improved password usability and security. One of the most important merits of graphical password is that they are simpler and better to remember compared to traditional alphanumeric. Humans have the memories and ability to remember places they have been to; things they see in the environment and faces they have seen for over a period of time [7]. The different methods used for graphical password schemes such as knowledge based which include recognition-based, cued recall-based and pure recall-based. Recall-based requires reproducing previous image drawn and sketching out the drawing by using a mouse or stylus on grid. While recognition password requires memorizing image at the time of password creation, and also recognize the picture images at the time of authentication. On the other hand, cued recall password scheme mostly offers a set of picture image and have to recollect and specifically aim at a location on a given image.

Graphical authentication scheme offers a user-friendly password interface and at the same time it increases level of security [8]. According to [9], Graphical based authentication password by Grey E. Blonder surface as the only option knowledge-based scheme except the alphanumeric password approach. Presently there some existing large number of graphical schemes. [2] Defined the term graphical password scheme as authentication scheme which operates by getting the user to choose from picture images, in a sequential manner and present them in an interface. It is for this fact that authentication technique's graphical pictures are utilized as password. This can be referred to as graphical authentication. [10] proposed an authentication algorithm as an option of traditional based authentication. It was accepted for the fact of humans can memorise picture images than the text. Therefore, graphical user authentication has been deemed to have higher usability and security than traditional authentication. Graphical authentication password is hard to break or infiltrate it by using normal attacks as in the traditional authentication and provides higher security level of graphical user authentication compared to traditional techniques. According to [10] The two classes of graphical algorithms techniques which are likely alternative to traditional password are recall and recognition based algorithms. Recognition based functions by users clicking the correct image in a particular order from the collection of images displayed to the user. According to [11], in the arena of information systems, the data security and information are of very great valued and importance. The data security revolves around technology which guarantee that integrity of data information is secured from manipulation or non-intentional change to original text, non-authorization to control access and accessible to grant the clients on the demand. An electronic system should have all the required security features as mentioned above. Any e-payment system that does not possess a secured feature

should not be trusted by the clients. Also, trust is of paramount importance to guarantee the acceptance of the electronic payment system by the clients. For us to have secured, a perfect and effective electronic payment system, a graphical based authentication method is employed. Therefore, this paper presents a comprehensive survey of graphical based authentication methods for an electronic payment system.

2. RELATED LITERATURE

A. Survey Approaches

In this paper, the survey is basically on graphical password scheme that is knowledge based with a move toward analyzing the various graphical authentication techniques currently in use. We will employ the use of knowledge based authentication schemes as an approach. Several graphical based password techniques have been proposed by various researchers in order to solve the demerits (setbacks) of alphanumeric or conventional textual password techniques, as the picture images are much easier to memorize than the text based password. In this comparative survey analysis will considered based on Algorithms (methodology), merits (advantages), demerits (drawbacks), security and usability. There are currently different survey approaches in graphical authentication passwords (scheme) for electronic payments. These approaches include: Recognition, Recall/Pure Recall, Cued Click Recall and Hybrid techniques respectively.

B. Categories of Graphical Authentication Passwords

Various techniques over the years have been identified. The most popular one amongst others is knowledge based scheme, which is rated most important technique in terms of security and usability. This technique have proposed to resolve quite number the setbacks of traditional password techniques, the reason is that the picture images are so much simple to recognize, memorize and better to recollect compared to text as presented in Figure 1 [7]. Currently, some existing graphical passwords authentication techniques are generally categorized into four main types as follows [7]:

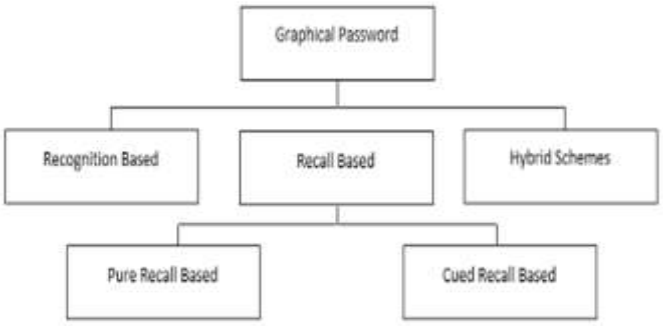

Figure 1: Categories of graphical password authentication techniques [7]

i. Recognition Technique:- recognition technique is one in which users choose images and symbols within a group of picture images. During the stage of authentication, it is required to recollect the chosen images or signs that were chosen earlier at the registration time, within the set of picture images.

ii. Recall Based Technique:- Recall based is quite simple and pleasant to use, only that the clients do not remember easily passwords. Although it is better secure compared to recognition technique.

iii. Cued Recall Technique:- Cued Recall scheme provides clients with a clue or hint. This clue or hint normally assists the clients in reproducing their password conveniently, efficiently and perfectly. Its operation resembles that of the recall schemes but nonetheless the scheme combines recall and cueing.

iv. Hybrid Schemes:- This scheme is popularly called hybrid technique. It is so called because a user combines one technique with another to form a single scheme, so as to resolve demerits or setbacks in one scheme like shoulder surfing and spyware attacks. Hybrid authentication techniques usually take care of the most common setbacks.

Recognition Graphical User Authentication Schemes:-

The various examples under the Recognition based graphical user authentication algorithms types are explained as follows:

1. **Awase E Algorithm:-** It is an algorithm where people needs to select and register with the system images tagged as "pass images". Upon authentication, series of images arrange in their

order will be displayed. If the picture object appears in the grid, then one will be required to "choose pass image", If the images are not displayed in the grid then one will be required to choose the "no pass image". This can be utilized as trick images. The procedure or authentication is reiterated for certain number of times in a random manner. This system does not allow for zero number of pass-images during an authentication stage which means that at least there will be a pass-image shown in one of the authentication stages. The position of the pass-image and decoy image on the grid of images is randomly chosen. Awase E permits one to input own image, which is described as setback (demerit) in the algorithm, as users have the habit of selecting favourite picture images that is liable to attacks, particularly those attackers who are close and are in position of client's data [22].

2. **Passfaces:** - Passface is a business product of Real Clients Corporation that requires select a face from the grid of picture faces displayed. One of the main merits of passface is that it is difficult to hack and to be distinguished or recollect. Here a user will have to select four human faces from the grid with nine pictures prior to completion of authentication procedure. The main demerits of this scheme are that people usually select faces by considering their characteristic similarities, also the login process could become unpleasant and face blind people cannot use the PassFaces algorithm [4, 12, 13].

3. **Déjà vu:** - Dhamija and Perrig [16] in Year 2000 proposed an algorithm refer to as Déjà vu. This requires a user to pick specific number of pictures out of huge picture images strictly on visualization technique. At the process of authentication session, user is required to identify selected picture upon which the user is then authenticated. Dhamija and Perrig claimed that this algorithm offers a better security because of its unfeasible writing the authentication key due to the fact that conceptual images are not easily described in words [14, 15, 16, 17]. The disadvantages of this algorithm are that due to the large number of images to be loaded in the database and also the authentication procedure is sometimes being lengthy.

4. **Triangle:** - [18] In his research work, proposed triangle method as a solution to shoulder surfing setback. Here the user requires picking pass-images selected at the registration phase within the group of images displayed. It is required by the user to click the inner side of the convex bull, which outlines the objects. [18] Recommend that the images or objects shown during the login procedure have to be elevated to a thousand (1000) images to allow the password space is reasonably bigger and hard to predict. It also suggests only three (3) pass-objects ought to be erratically spread all over the screen and the objects have to vary from each other, so as to allow user differentiate objects. The setback is that if the numbers of objects shown are too many then it will be extremely hard to know the pass-objects and also if the objects shown are little, then the password space will turn out to be smaller, so this will be simpler to predict and break [10, 19, 20].

5. **Story Algorithm:** - This scheme was proposed by [21], that a user can selects his own password in mixture of 9 types to make single Story. These types will have to be different and be a derivative of the group that shows users daily life, for example cars, pets, food, etc. It is required to choose a particular size of images, which were the chosen images at registration time. This means that it is only when the sequence of picture images is right, otherwise the user is authenticated. Its main setback is that it is difficult to remember the order of images compared to pass-faces method.

6. **Picture Password:** - Jensen et al [22, 23], in their research work, suggested the algorithm is particularly develop and put into operation for portable devices (mobile). The user chooses theme such as cats, dog etc at registration stage. This theme is made up of thumbnail photos, registered in sequential order of images as password. At the registration stage, the user will have to use stylus to register order of the images within the theme to create password for authentication. It Setback is that the size of thumbnail photos is narrowed to thirty (30), so the number of password space is regarded as minimal, and each thumbnail photo is given a number and order of image chosen will generate a numerical password space larger. Jensen et al in their work indicated that user can choose two or more thumbnail photos within the same period of time to form new numerical component. Its setback is that the newly formed password turns out to be complicated and hard to recollect or unforgettable.

7. Colour Login Algorithm: - [24] The background colour of this algorithm is applied in order to reduce the login time. Also, the presence of multi-colour is made confuse fraudsters but it is simple for user authorization. The algorithm is resilient to shoulder surfing attacks. The demerit is that it has less password space compared to alphanumeric or text password [25].

8. 3-D Password Algorithm: - This algorithm allows users alternative to select a mixture of authentication models. For example, a mixture of recognition, recall, biometrics, and token type of authentication that will interact among objects. As a result of huge number of choices, the attacker will find it difficult to penetrate or encroach. The users have the freedom to select any one or join the techniques (models) together. The ability to memories and robustness against guessing attack could not be able to written down or trespass by social engineering attackers, so part of their goal is that it is not hard for them to reverse or cancel the password. 3-D password algorithm has large password space and so it is used in high security application systems, for example, armed forces installations or central databases.

9. Convex-Hull Technique: - Convex-Hull technique is used to solve shoulder surfing setbacks. Here the user needs to pick k icons within the N icons, which the scheme will display on screen during the registration. These, quite a number of scenes are being displayed to the user during the login and the user needs to choose j icons such that 3 is less than j and j less than k, and then click the inner side of the convex-hull formed by I pass icons. The two main important setbacks of this technique are the sluggish process of login and its small password space [1, 26].

10. Random Geometric graphical password (RGGP): - The aim of this scheme is to resolve setbacks of image password, that can simply be predicted due to their close similarity. if closely related picture images are used, then there will be shoulder surfing and phishing attack. The scheme is assumed to be secured for the following reasons: **i.** its huge number of password space makes it to be resilient to Brute Force Attack, **ii.** Its complex geometric nature makes it strong resilient to fraud by social engineering and shoulder surfing, **iii.** Adequate caution given by the arrangement of objects to stop user from getting into the websites, **iv.** Picture images can be readily formed when it is needed. This technique is a click points based that reminds users of the actual location clicked during the registration procedure. The security analysis of this technique proved that in brute force search the password space is larger compared to those in textual password. The main merit of this technique is that it is resilient to guess and forgery attacks due to tracks and randomly generated colours. It is also resilient to spyware as they cannot narrow the mouse clicks [26]

11. Jensen et al Technique: - [2, 24] proposed this graphical technique mechanism for portable devices (mobile) and PDAs. Here a user needs to pick a theme, for example dogs, cats, rats etc. The theme images are displayed to users in the grid of 5 x 6. Also, every image is shown in thumbnail number. In order to create password a user needs to choose image in an orderly manner. Then the user will have to recollect the earlier images chosen and pick the image by the use of stylus in an accurate order for authentication. In this technique the images are narrowed to 30 making the password space size to be relatively small. A numerical value is allotted for every image and a sequence will be chosen to form a numerical password. At some point, the numerical usually are less compared to text password. In order to surmount these, two images can be chosen at same time using one click to raise the password space number. But the setback of this, is that it will create complexity and tough or hard for user.

12. VisKey Algorithm: - In VisKey algorithm, the user is required to hit spots where their prearranged image in order to be authenticated. The algorithm is a commercialised one in Europe specifically in Germany [22]. It was particularly made for portable devices such as smart phones, iPad, Tablet ect. The algorithm grants and allows input at a given tolerance region of the picture image to curtail the difficulties in getting the accurate spots. It also gives the user an alternative to decide size of the region. The disadvantage of this is that the input accuracy requires careful setting as it causes direct influences on security and usability of the password.

13. Where is Waldo: - [22, 27] In their research work, indicated that to overcome the setbacks of shoulder surfing, the algorithm needs

to permit a user to choose a number of images as pass-objects. Here every object has numerous variants with a distinct code to each of them. At the authentication session, the user encounters different scenarios. Every scenario has numerous pass-objects and decoy objects. Since the code is distinct, then the user can enter sequence of code as his or her password and code similar to the region of the pass-objects with reference to a pair of eyes. This algorithm also requires the user to memorise textual code of every pass-object variant. Hong et al, who are researchers, expanded Where is Waldo algorithm to give the user's ability to choose own codes. In order to arrange the picture images [25], he utilizes a grid-based array and erratically generated images shown on the screen each time during the login procedure. Its demerits are [24, 26], the approach is time wasting and consuming, and so, it is discouraging as a choice by quite number of users.

Recall based Graphical User Authentication Algorithms

There are two types of Recall Based Graphical User Authentication algorithms. These algorithms are Pure Recall Based and the Cued Recall Based. There also various examples of algorithms and these include the following:

1. **Grey E. Blonder Algorithm:** - Blonder in the Year (1996) [15, 22, 26] proposed this algorithm where a user is offered an image selected at the time of registration process. At this phase he selected a hit region or a location within the picture image. At authentication session, a picture image is shown for user to click on the regions in a prearranged manner for authentication. The main merit is that it is extra suitable to use compare to text-based password. Demerit of this scheme is related to the memorable password space. Also, number of reference clickable regions is comparatively tiny and therefore, the password is quite lengthy to secure, it has a simple image background [25].

2. **Pass Points:** - This algorithm was developed by [28, 29], it was essentially expanded by Grey Blonder's technique removing the predefined margins and also the removal of synthetic images that could be used. The algorithm allows user to selects various regions on the image in an order of sequence. To create a password during registration, users have to click any region on the image. At the login a user is required to click the close place on the chosen click point and then the tolerance of every selected click point will be calculated. For the authentication a user needs to click around the tolerances of the selected click regions in order of sequence. The setback is that password is simply formed but users will find it hard to learn passwords compared to textual. The login time is much bigger compared to text based password.

3. **Passlogix V-Go Technique:** - The technique is a commercial incorporated coy in the USA. The technique (algorithm) is referred to as "Re-iterating sequence of procedures" meaning forming of passwords by moving through an image repeatedly. Some of the setbacks of this algorithm is that the password size is relatively small, passwords here can be guessed or predicted.

4. **Draw A-Secret (DAS):** - In this algorithm, [27] the researcher proposed a technique where user draws a sketch of a picture in 2D grid of G x G. In this technique each grid has a rectangular shape with coordinate x and y. Here the values of the grid are being stored in sequence of which they are drawn. At authentication, he or she has to re-draw exactly same picture to touch same coordinate's grid. Its merit is that the password space is better and more enhanced than text based password. Also, its setback is the choice of weak drawing which is vulnerable to dictionary attack.

5. **Grid Selection:** - In the research work of Thorpe and Ooschot in Year 2004, they made improvement on DAS by learning the effect of stroke count that reduces with little strokes on the grid. The setback of this algorithm is that users cannot recall stroke order, it is non resistant to brute force, guessing and spyware attacks. Its merit is that it is resistant to dictionary and shoulder surfing attacks. Also, the demerit of the algorithm is that it carries same setbacks as Draw A-Secret (DAS) [22].

6. **Passdoodle:** It is an algorithm that is related to DAS. It allows a user to freely form a drawing to serve as password without seeing a grid. Goldberg et al analysed a small paper based study of Passdoodle which revealed that user can remember the final drawing but made mistakes in the recall of the figure, sequence or the direction of the pen strokes. Also, anytime the user requires to be authenticated, he has to write doodle password. [15, 30] has proved theoretically that as

a result of huge feasible numbers of doodle password, the algorithm was much harder to break. [31, 32] in their studied work, finalized that users were able to recognize a full doodle password correctly as textual password. One of the demerits is that users are captivated by other users and it is vulnerable to attacks, such as shoulder surfing, guessing and spyware.

7. Syukri Algorithm: [7] in this algorithm, a user is required to draw own signature using mouse. The algorithm does not require user to memorize the signature drawn. It has two phases namely, the verification phase and registration phase. One of the merits is that it is hard for the attackers to forge and it is more suitable for smart phones and other devices that possesses stylus. Also, the demerit of this scheme is that it is not comfortable for the users to use mouse to write their signature.

8. Quantitative DAS Algorithm (QDAS): This algorithm is an improved graphical scheme of DAS where every stroke is coded and was formed. The QDAS provides larger password space compared to DAS technique. The demerit of the scheme is that it is harder for users to recall the sequential order compared to the original DAS technique. Its merit is that it decreases the setbacks of shoulder surfing.

9. Background DAS: This algorithm was created in 2007 by Dunphy and Yan [5], they in addition insert background picture-images to Draw A-Secret, in order to enhance and create stronger passwords. Also, the significance of the background is that it is much better for recalling. The demerit of this technique is problem of shoulder surfing and the interference of the large password space. Its merit is that the background image decreases the quantity of symmetry that causes the lengthy passwords.

10. PassMap: This algorithm uses a Map for password authentication. PassMap has both registration and authentication phases. In the registration procedure, the user is allowed to select a Map, (for example; World Map, Map Africa or any country) and the user will pick either States, Cities or a country he wants to visit or have visited in recent times. This algorithm will authenticate a user if he or she accurately identifies the selected point on the Map. Its setbacks is that it is vulnerable or prone to Brute Force search and Dictionary attacks. It is simple and convenient to use and resistant to shoulder surfing.

11. Pass – Go: It is advancement to Draw A-Secret (DAS) algorithm. Pass-Go algorithm was created in the Year 2006. Pass-Go uses grid based technique that needs a user to choose intersections rather than cells. It is simple creation and clickable point. It is resistant to Brute Force.

3. FINDINGS

In the course of this Survey research work, the aims are to identify the different Graphical Based Authentications with the view to evaluating these graphical authentication algorithms to determine the best performance on the electronic payments depending on the feature criteria pattern or approach specify for the algorithms for authentication accordingly. The followings are findings on the recall-based user authentication algorithms:

a). Blonder:
Usability: Mouse usage, Clickable Points, Memorability, Simple Steps, Simple Training.
Merits: It is resistant to Dictionary attack, Spyware, Description.
Demerits: Password space is relatively small. It is non resilient to brute force, guessing, and shoulder surfing attack.

b). PassPoint:
Usability: Mouse Usage, Clickable Points, very memorable, it has simple steps, it has attractive interfaces, it has simple training operations tools, it is satisfying, enjoyable, and lovely picture images.
Merits: It is resistant to Dictionary attack, Spyware, Description.
Demerits: Longer than alphanumerical method, Difficulty in memorizing. It is non-resilient to brute force, predicting and surfing attack.

c). VisKey:
Usability: Mouse Usage, Clickable Points, a memorable scheme, simple and easy steps, attractive interfaces, simple and easy training operations, and lovely & amusing/satisfying picture.
Merits: It is resistant to Guessing, Shoulder Surfing and Brute Force.
Demerits: Input tolerance/precision. It is non resilient to dictionary, spyware and description.

d). Passlogix V- Go:

Usability: Meaningful, Memorability, Nice Interfaces, Pleasant Picture.
Merits: It is resistant to Brute Force
Demerits: Small password space due to limited length of activity. non-resilient to Spyware, Dictionary, Description and Guessing.

e). Draw A-Secret:
Usability: It uses mouse, Simple Steps, Simple Training.
Merits: Resilient to Dictionary and shoulder surfing attacks.
Demerits: Users cannot recall stroke order. It is non resilient to Brute Force Search, Spyware, Description and guessing.

f). Grid Selection:
Usability: It uses mouse, Simple Steps, Simple Training.
Merits: Resilient to Dictionary and shoulder surfing attacks.
Demerits: Users cannot recall stroke order. It is non resilient to brute force, guessing, description, guessing and spyware.

g). Passdoodle:
Usability: Stylus usage, meaningful, Simple Steps, Simple Training.
Merits: It is resistant to Dictionary, Shoulder Surfing.
Demerits: Cannot recall the order of drawing doodle, it is non-resistant to Brute Force, Guessing, Description.

h). Syukri:
Usability: Meaningful, Memorability, Simple Steps, Nice Interfaces, Simple Training.
Merits: Resistant to Dictionary, Shoulder Surfing.
Demerits: Not every user can draw with a mouse; it is Non-resistant to Brute Force, Guessing, Spyware, Description and Guessing.

i). QDAS:
Usability: Mouse usage, Simple Steps, Simple Training
Merits: It is resistant to Dictionary, Shoulder Surfing,
Demerits: It is less Memorability that DAS, it is non-resistant to Brute Force, Guessing, Spyware, Description

j). BDAS:
Usability: Mouse Usage, Meaningful, Memorability.
Merits: It is resistant to Shoulder surfing, Dictionary,
Demerits: There is interference between passwords; it is non-resistant to Brute Force, Guessing, Spyware, Description.

k). PassMap:
Usability: Mouse Usage, Meaningful, Clickable Points, Memorability, Simple Steps, Simple Training.
Merits: It is resistant to Shoulder Surfing, Guessing.
Demerits: Users can forget the particular chosen order, it is non-resistant to Dictionary, Spyware, Description, Brute force.

l). Pass Go:
Usability: Simple Creation, Clickable Points, Memorability, Simple Steps, Nice Interface, Simple Training,
Merits: It is resistant to Brute Force, Guessing
Demerits: Error tolerance mechanism due to no boundaries on the intersections, it is non-resistant to description.
The following are also findings on the recognition-based user authentication algorithms:
a). Convex-hull Scheme:
Usability: it requires training to memorise faster, it is a good usability
Merits: it is resilient to shoulder surfing, randomly clicking and rotating.
Demerits: it possesses low login process, password space is probably small
b). 3-D Password:
Usability: Memorise easily, good Usability
Merits: It is resilient to guessing, Social Engineering, Easy to change & cancel password, It has large password space.
Demerits: The scheme is still not resilient against shoulder surfing attack; it is non-resistant to shoulder surfing.
c). Colour Login technique:
Usability: The background colour decreases the login time and many colours in the technique helps to confuse the imposters
Merits: The algorithm is resilient to attacks such as shoulder surfing
Demerits: Its password space is quite lower compared to textual password.
d). Jensen et al technique:
Usability: meaningful, it is organized by theme, image is assigned, easy and fun to use, the algorithm uses stylus in the accurate in sequential order in authentication. User is allowed to choose

simultaneously 2 picture images on only one click to elevate the password number.
Merits: The users are allowed to choose and register order of the thumbnail photo chosen to create password
Demerits: Picture image in this algorithm are narrowed to 30, the password space are relatively small, algorithm is non resilient to brute force search.

e). Random Geometric Graphical Password (RGGP).
Usability: Algorithm is simple to recall, it's difficult to predict by attackers, the images can be created fast, and it does not need any database to store images.
Merits: The algorithm is resilient to predicting attack, resilient to manipulations (forgery) attacks and surfing attacks, Phishing, Brute Force, Social Engineering, Spyware and it is key loggers resistant.
Demerits: It is not applicable

f). Déjà vu:
Usability: Its mouse usage, it is simple in password creation, its assignable image, it has simple steps and simple training
Merits: The algorithm is resistant to description, dictionary, spyware and brute force.
Demerits: It has long authentication process; it is a non-resistant to guessing and shoulder surfing.

g). Moving Frame:
Usability: Mouse usage, Simple Creation, Memorability, Simple Steps.
Merits: The algorithm is resilient to shoulder surfing, spyware and description.
Demerits: Algorithm is time consuming and unsatisfactory process, non-resilient to dictionary, description and shoulder surfing.

h). Where is Waldo:
Usability: Simple Creation, Assignable Image, Memorability, Simple Steps, Simple Training,
Merits: The algorithm is resistant to brute force, guessing and spyware
Demerits: Memorizing each alphanumeric password code and process is time consuming; it is non-resilient to dictionary and Shoulder Surfing and description.

i). Awase-E:
Usability: Image is assignable, Simple Steps, Simple Training, Memorability.
Merits: Resilient to Brute Force and Shoulder Surfing
Demerits: Allows users to choose own images which they are likely to select favourite images that is prone to attacks. It is non-resistant to Description, Guessing

j). PassFaces:
Usability: The algorithm is assignable picture image, it is memorable, simple steps, lovely and attractive interface and also simple training and satisfactory picture
Merits: It is resistant to Spyware, Description
Demerits: Password based on culture, race and gender, and can't be used by facially blind people. It is non-resistant to Dictionary, Guessing, Shoulder Surfing and Brute Force

k). Story:
Usability: It is meaningful, assignable image, memorable, it has simple steps, attractive and lovely interface and satisfactory picture
Merits: It is resistant to Spyware and Description
Demerits: It is difficult to remember sequence of authentication; the algorithm is non-resilient to Shoulder Surfing, brute force and Guessing

l). Triangle:
Usability: Mouse usage, Simple Creation, Memorability, simple steps
Merits: It is resistant to Dictionary, shoulder surfing, Description
Demerits: Large number of displayed objects makes it difficult for user to identify pass-objects. non-resilient to Brute Force and Guessing.

m). Picture Password:
Usability: Its Mouse usage, Simple Creation, assignable image, memorable, simple steps, attractive interface, simple training operations, satisfactory and lovely pictures.
Merits: it is resistant to Brute Force and Guessing
Demerits: Password space is small due to a limited number of photos to 30. It is non-resistant to Shoulder Surfing and Spyware.

4. RECOMMENDATIONS

In this survey study, 13 recognition based and 11 Recall based Graphical Authentication techniques have been elaborately analysed accordingly. As for recognition based authentication algorithm, the most common drawbacks were that the process of authentication is usually long or time consuming and also that the process was usually complex. Also, the security attack on most of the algorithms are most prone to is "Guessing" and

the security attack that most of the recognition-based algorithms are resistant to are "Brute Force, Shoulder-Surfing and Description Attacks." Some of the major demerits (setbacks) found in pure recall authentication scheme is that a user will simply not remember sequential order needed for him to authenticated. Again, majority of the users usually select weak picture images as password. Hence the most prone attacks to users in the recall-based algorithms are "Guessing and Brute Force" and the most resistant security attacks are "Shoulder Surfing and Dictionary". Since Recall-based is most prone to Guessing and Brute force attacks and Recognition-based is most resistant to Brute force. Therefore, future studies must be ready on accepting the mechanisms being used in recognition based and also apply it in the Recall-based. The authentication procedure would make it quicker and will be more efficient in preventing guessing. The clients should be trained or educated on the usage and ways to select hard picture images as password.

5. CONCLUSION

To conclude, our survey has analysed 13 Recognition and 11 Recall based graphical authentication schemes based on their usability, characteristics, merits, demerits or setbacks, and security attacks (prone and resistant). Recommendations have been made to address some of the security issues facing these authentication schemes. Shoulder surfing, Description and Dictionary are the attacks most resistant to these authentication algorithms.

6. FURTHER STUDIES

Finally, this research has systematically conducted a broad study on existing researched works on Graphical Authentication Schemes and a comparative analysis of the various algorithms surveyed indicates that graphical authentication scheme is more hard for hackers when traditional attack methods are used, such as Brute Force, Dictionary, guessing, shoulder surfing, social engineering and spyware attacks. In general, the current graphical password techniques have given much fair level of security and usability. However, advance research and broad studies for graphical schemes are much more required so as to achieve greater levels of maturity, much stronger Security development technique as well as its usefulness.

7. REFERENCES

[1] H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System," IEEE Trans. Dependable Secur. Comput., vol. 15, no. 2, pp. 180–193, 2018.

[2] T. Akram, V. Ahmad, I. Haq, and M. Nazir, "Graphical Password Authentication," vol. 6, no. 6, pp. 394–400, 2017.

[3] G. M. Mayuri, S. V. Krishna, and M. Tech, "Graphical based Secure Authentication System for Online Applications," vol. 4, no. 8, pp. 2868–2872, 2013.

[4] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," Proc. - 2nd Asia Int. Conf. Model. Simulation, AMS 2008, pp. 396–403, 2008.

[5] K. Ritu, R. R. Singh, and B. Kumar, "Comparative Analysis of Recall-based (Drawmetric) and Click-based (Locimetric) Graphical Password Authentication Schemes," vol. 6, no. 2, pp. 1573–1577, 2015.

[6] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical User Authentication System Resistant to Shoulder Surfing Attack," vol. 19, no. 4, pp. 1–8, 2019.

[7] D. Kadu and S. Therese, "Different Graphical Password Authentication Techniques," no. March, pp. 56–58, 2017.

[8] S. H. Dogo, "AN IMPROVED MAP BASED GRAPHICAL ANDROID AUTHENTICATION SYSTEM," vol. 13, no. 1, pp. 23–27, 2018.

[9] M. Ahsan and Y. Li, "Graphical Password Authentication using Images Sequence," no. December, 2017.

[10] S. A. Razvi, "Implementation of Graphical Passwords in Internet Banking for Enhanced Security 1," pp. 35–41, 2017.

[11] M. Masihuddin, B. Ul, I. Khan, M. M. Ul, and I. Mattoo, "A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts," vol. 10, no. May, 2017.

[12] M. Thirunavukkarasu, "An Improving Method of Grid Graphical Password Authentication System," vol. 7, no. 5, pp. 40–43, 2017.

[13] T. Khodadadi, A. K. M. M. Islam, S. Baharun, and S. Komaki, "Evaluation of recognition-based graphical password schemes in

terms of usability and security attributes," Int. J. Electr. Comput. Eng., vol. 6, no. 6, pp. 2939–2948, 2016.

[14] V. Rathanavel, "Graphical Password as an OTP," vol. 6, no. 1, pp. 1–6, 2017.

[15] M. A. Khan, I. U. Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices," IEEE Trans. Consum. Electron., vol. PP, no. c, p. 1, 2019.

[16] K. Olamide and I. Remo, "Shoulder Surfing Resistant Graphical Authentication Scheme for Web Based Applications," 2017.

[17] N. S. Zabidi, N. M. Norowi, and R. W. O. K. Rahmat, "On the Use of Image and Emojis in Graphical Password Application," no. 8, pp. 379–385, 2019.

[18] F. Sepideh, "Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing , Smudge and Brute Force Attack," vol. 13, no. 12, pp. 616–620, 2019.

[19] E. Yesseyeva, K. Yesseyev, M. M. Abdulrazaq, A. H. Lashkari, and M. Sadeghi, "Tri-Pass : a new graphical user authentication scheme," no. June, 2016.

[20] A. Ahmad, M. Asif, M. K. Hanif, and R. Talib, "Secure Graphical Password Techniques against Shoulder Surfing and Camera based Attacks," vol. 14, no. 10, 2016.

[21] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT | A novel graphical randomized authentication technique for consumer smart devices," IEEE Trans. Consum. Electron., vol. 65, no. 2, pp. 215–223, 2019.

[22] E. Ekeke, K. Ugochukwu, and Y. Y. Jusoh, "A Review on the Graphical User Authentication Algorithm : 2. Categories Of Graphical User Authentication Algorithm," Int. J. Inf. Process. Manag., vol. 4, no. May, pp. 238–252, 2013.

[23] I. Journal, S. Issue, S. Veerasekaran, and A. Khade, "USING PERSUASIVE TECHNOLOGY IN CLICK," vol. 31, no. 31, pp. 29–36, 2015.

[24] A. S. Gokhale, P. Vijaya, and S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," Procedia - Procedia Comput. Sci., vol. 79, pp. 490–498, 2016.

[25] P. Saranya and S. Sharavanan, "AUTHENTICATION SCHEME FOR SESSION PASSWORDS," no. September, pp. 590–603, 2017.

[26] S. Farmand and O. Bin Zakaria, "Impro passwving graphicalord resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)," ICIME 2010 - 2010 2nd IEEE Int. Conf. Inf. Manag. Eng., vol. 1, pp. 644–650, 2010.

[27] M. Computing, "Comparative Study of Graphical," vol. 3, no. 9, pp. 361–375, 2014.

[28] V. Zimmermann and N. Gerber, "International Journal of Human-Computer Studies The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes," J. Hum. Comput. Stud., vol. 133, no. April 2019, pp. 26–44, 2020.

[29] M. Ashwini and K. C. Sreedhar, "Improved Persuasive Cued Click Points for Knowledge-Based Authentication," vol. 15, no. 11, pp. 95–100, 2015.

[30] S. Istyaq and K. Saifullah, "A New Hybrid Graphical User Authentication Technique based on Drag and Drop Method," no. October, 2016.

[31] H. U. Suru and P. Murano, "Security and User Interface Usability of Graphical Authentication Systems – A Review," no. February, 2019.

[32] H. Mathur and V. Lokhande, "Improved Pass-Matrix for Graphical Authentication," vol. 6, no. 2, pp. 140–143, 2017.