Middle-East Journal of Scientific Research 21 (11): 2039-2051, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.11.21781

JIGSPASSZLE: A Novel Jigsaw Based Password System Using Mouse Drag Dynamics

S.M. Udhaya Sankar and V. Vijaya Chamundeeswari

Department of Computer Science and Engineering,
Velammal Engineering College, Chennai, India

Abstract: The evolution of internet made people to access their data from the internet itself. Even most sensitive data are stored in the internet and are used many times. For such sensitive data there is a need to defend against the unauthorized access by implementing secure access management. In this paper we would like to propose and evaluate JIGSPASSZLE a novel image based authentication system which uses the ability of the human to recognize the image. JIGSPASSZLE uses a new biometrics system based on the human drag action either using the mouse or using touch in the screens. In our approach we will be displaying the One Time PIN in the screen itself, user has to remember the order of the image chosen by him and have to place in the numbered box. Our approach is using two level security systems. The first level is as usual which exists in majority of websites where user has to enter his text password. Then in the second level is to the place the images in correct order in which the user has ordered during registration. During this stage we will be getting the time taken by the user to submit his password. The combination of ordering the image and the time taken makes this stage more complicated to break.

Key words: User authentication · JIGSPASSZLE · Graphical passwords · Drag stroke

INTRODUCTION

If authentication systems are built without incorporating the knowledge of human strengths and limitations, then users will not use them or they will make errors in using them [1-7]. Users should not involve in actions which can compromise the authentication system and fail. In general nowadays we are normally using text based passwords. Mostly these passwords are static in nature and often requires human to remember them whenever they want to login. But people have the tendency to have easy passwords which are very easy to break. Weak passwords suffer from vulnerability to brute-force and dictionary attacks [8]. To make passwords dynamic and more secured, developers started to use the concept of One Time Password (OTP). They are only valid for exactly one authorization or authentication request [9]. Normally easy way to use OTP is to send it to mobile phones, while some send to another e-mail ID's when we login to other websites(eg:-E-commerce Websites). Recently, the online storage service Dropbox added SMS-based two factor authentication after facing some security issues [9]. But for this service there is an additional need of hardware both in the server side and in the client side. It is not possible for the clients to have additional hardware's all the time with them. And another drawback is the mobile malware Trojan which has the ability to steal the user passwords [10]. All these are normally installed by the user and use social engineering attack for stealing the information. During the text based password era to enhance the security, there was introduction of a biometric from pressing the keys in keyboard; they are normally called as Keystroke. Mostly commonly used Keystroke is static Keystorke which are used only during particular session, normally during the login time [11].

To replace the drawbacks of text based passwords, Graphical passwords are introduced. Graphical passwords are mainly based on user imagination and recognisation power. Human brain has the ability to store images quickly than text. So it will be very easy for the user to setup the password which is based on image rather than

Corresponding Author: S.M. Udhaya Sankar, Department of Computer Science and Engineering, Velammal Engineering College, Chennai, India.

setting up long text based passwords. Recently we can see the trend of more image based passwords like we have him Microsoft's Windows 8 PC, then Blackberry's BB10 image based password. These give the user very easy access to use. The ability of the user to recognize the picture which is related to him is very high than any other pictures which are usually not related to him. In such cases even when the pictures are made into slices the user can bring them into proper form very soon. On the other hand, system generated random images are proven to be difficult to remember [10]. So when we are designing the Graphical password it should be designed properly so that it is difficult for any computer programs to attack and get the password and at the same time it should be very easy for the user to use for very long time.

In this paper, we present JIGSPASSZLE a security system based on user image recognition power and the speed of recognizing the smaller parts of the image. During the registration process the user is allowed to upload his image which he find easy to use at any time. That image is divided in 9 (in 3X3 fashion) equal pieces. Then the user is allowed to arrange the pieces in the order he wants in linear fashion (1X9 fashion). The user is made to remember this order to enter into the system because it acts as the authentication. The idea behind the JIGSPASSZLE is that the user has the ability to find any part of the image quickly and can set the password faster than anyone. And only the user has the ability to remember the order which is made by him during the registration. During the time of login the user first needs to finish the first level of authentication, in the second level he is displayed with the unique One Time PIN (OTP). The number in the PIN is the position at which the images have to be placed in the correct order which is registered by the user. We tried to conduct test for this login system to a group of 15 students. Among that 80% found it very easy to use and they reproduced the passwords correctly even after a week. But some students found difficult to remember the order when the image had less content or which is not belonging to them.

Before explaining about our work we would like to discuss some of the basic things which are required to gain the knowledge about the security system.

Literature Survey: Adams, A. and Sasse, M. A. in their paper "Users are not the enemy "(1999) tells us how any authentication system should be designed properly. Each and every module of the authentication system should be very carefully designed and also it should not make the user to feel that it is not much secured. In the same time the user should be willing to use the authentication system for the long time. The user should not get bore after using each and every time. He shares that there are tendency for the human to give the passwords wrongly many times at that time also the authentication system should be able to response properly instead of stop working. Even when there are large number of request coming to the system there is need to work properly. Then he defines about the user interface design of any system. Whenever we design any interface which will be interacting with the user that interface should look visually pleasing. Choosing the colors for the user interface is very important. The interface should attract the user to use it. It should be in some ways addictive to the user.

Kulkarni. in his paper Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication (2013) tells us how the multi level authentication will be very useful. He also tell how the combination of both text based password and image based password will be very complex to break. Finally he introduces One Time Passwords which are generated each time when the user logins. He shows that such multi factor combination is very helpful and is not easily breakable. And also the usage of dynamic token during login (OTP's) makes the system unbreakable. In this paper they tells us that the computer bots will find it very difficult to crack the multi level authentication factor. Because the bots are usually designed for any specific thing like text based password or image based password. In the multi level authentication systems the bots should have lot of analysis power to identify what type of authentication are used in several levels. First they might have used text based authentication alone, then image based authentication then may be Token based authentication. They are in need to analysis which will take more than.

Some of the white paper from famous security based companies like Symentec, Mcafee show that multiple factor authentication in the single level of authentication is very good and proved to be very effective in the authentication system. The famous example for multiple factor authentication is Google's Two step verification. Here after entering the username and password the server will send OTP to the hardware. And the user needs to enter the number which he gets to his mobile in the web interface. Here there is a dependence of the mobile. Another multiple factor authentication can be seen in the Key stroke based password. Here the users need to type

their password properly and correctly. Then at the same time the time of each and every type is counted in the back and stored and later the values are compared with the existing values in the database.

Mrs. D. shanmugapriya and Dr. G. Padmavathi, in their paper "A survey of Biometric Keystroke Dynamics: Approaches, Security and Challenges (2009) shows us what are the different types of biometrics based passwords can be achieved with the help of the Key stroke and what are the various Security issues we will see when we use keyboards and the challenges in implementing the biometrics based passwords. From this we can gain that biometrics based passwords are more secured when it is not able to capture the biometrics. They showed that keystrokes are normally can be reproduced easily with the help of small piece of software programs. And with the help of the keyloggers the text passwords are captured. There are lot of software which can capture both the time taken by the human to enter the password and also what the password he has typed. These software will send the data to the required destination without the knowledge of the user. The attacker can easily by pass the authentication.

Rohit Ashok Khot (2011) in his paper MARASIM: A Novel Jigsaw Based Authentication Scheme Using Tagging, shows that how the image based authentication will be very easy for the user and how it will be helping the search engines to find the different object from text. He clearly shows what are the different image based authentication and all the previous work made by the researches for developing the image based authentication. Graphical Passwords: A Survey by Xiaoyuan Suo, Ying Zhu G. and Scott. Owen clearly shows us the various loop holes in the existing graphical passwords. They have shown that most of the graphical passwords are easily attacked. Mostly attacks like shoulder surfing, brute force and Dictionary attacks are happening on graphical passwords. They suggest that these attacks normally happen due to thinking capacity of the user. Where the users have the tendency to choose very famous pictures and easy pictures as password.

Nitisha Payal, Nidhi Chaudhary, Parma Nand Astya in their paper "JigCAPTCHA: An Advanced Image-BasedCAPTCHA Integrated with Jigsaw PiecePuzzle using AJAX" (2011) shows how the small piece of image will be very helpful in stopping DDOS(Distributed Denial of Service) attacks in long run. They have stressed on several points like how the images are to be transferred and what are the best ways to store the images in the database and retrieving them. They have told that storing the images directly into any database table will affect the performance of any database. Rather than it will be really good to store them in the webservers and then in the database tables we can store the path where the data are stored. This will be very helpful during the time of taking backups and also optimization. They have also told about loading the images from the databases. When we load whole all the parts of images at the same time it will be very difficult and it will take lot of time. In such conditions the user will get bored and angry to use the system. Instead of that we are in need to load the images by using AJAX (Asynchronous Javascript and XML calls) i.e. we need to load the images one by one. So the users will feel that the system is working properly and so they can wait for sometimes to completely load.

Mori, T. Uda, R. and Kikuchi, in their paper "Proposal of Movie CAPTCHA method using Amodel Completion" tells how in any image based system we can avoid attacks from the bots. They have proposed a system where the images should be properly split into several parts. And we need to define each and every part a specific difference which will be very hard for the bots to understand. They shown when the images are slightly moving the possibility for the bots to scan the images will be very difficult and it will be easy to prevent the DDOS attacks. And along with moving images we are additionally need to give some differentiating colors to the parts of the images which will be helpful from preventing DDOS attacks. But adding colors may be harmful at some point of time. So it will be good to avoid for such image based systems.

Farnaz Towhidi and Maslin Masrom in their paper "A Survey on Recognition-Based Graphical User Authentication Algorithms(2009) mentioned how the image based password should be. They have told in detail how the Recognition based Graphical authentication will be helpful to the user and how easily they can help the user to finish the authentication process. They have clearly told how recognition system will be working and what will be the drawbacks in other image based authentication systems. They have concluded that for user friendly image based authentication it should be purely recognition based in nature. And they have also mentioned that using the private images which are from the users will be easy for them to use the authentication and also it makes difficult for computer bots to scan them.

Saurabh Singh and Dr. K.V.Arya, in their paper "Mouse Interaction based Authentication System by Classifying the Distance Travelled by the Mouse" (2011)

told how a mouse interaction can be used as a authentication system. They have mentioned about how the mouse interaction will be differentiated among different users. They have also made a study about the various mouse interaction like clicks, drags, mouse rotation and click & drop. They have formulated the biometric system from this study and also showed how well it will work. They have told about various dimension in the clicks and in detail they showed how it will be varying from user to user.

Related Work: Based on the cognitive activity required to remember the password, we divide the graphical password schemes into four different categories [12]: Pure Recall, Cued Recall and Recognition based techniques.

Pure Recall-Based Technique: In this type of technique there won't be any hint or remainder. The users have to purely remember what the password is and he has to reproduce it when required. These type of passwords are considered as most difficult to crack and difficult for user to reproduce. Some of them are Passdoodle; Draw a Secret, Grid Selection and Syukri Algorithm. In these the user either has to draw any shapes or they have to give their unique signature with the help of the mouse or stylus on the screen. For example in Passdoodle we need to draw the pattern in the touch sensitive based screens. And in Draw A secret we need to draw a pattern in the grid the points traced by us are located and in Syukri Algorithm we need to give our signature for entering. But in general having touch based screens is little bit difficult and we need to have additional hardware as stylus is difficult in current time. And for Syukri algorithm it is extremely difficult to draw the signature with the help of the mouse. Not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn [13]. It is also very difficult for the user to remember and reproduce exactly what he has drawn and the position where he has drawn.

Cued Recall-Based Technique : In this type of technique, a framework is proposed for reminder and for hints and gesture which will be helping the user to reproduce their password in accurate manner. Some of them are as follows VisKey SFR, Passlogix v-Go, Background DAS (BDAS), PassPoint, PASSMAP and Blonder. In Blonder the user is presented with a pre-determined image and has to click on the pre-determined position in the order he chose. While in Passpoint we can use any natural picture or painting and works similar to Blonder. In VisKey SFR the user needs to taps on the certain points in predetermined order. Here in Blonder we have the very less possibilities which are overcome by Passpoint, but the image we choose should have large number of different points while in VisKey SFR the problem is with input fault tolerance. The users find it difficult for finding the exact points in the screens. PASSMAP ask the users to remember the landmarks from the map he has visited while the Passlogix v-Go allows us to choose the password depends on the place in the home or office. But the password system several affected by the Brute force attack and PASSMAP finds it difficult for the user to remember [13].

Recognition Based Techniques: In this type of techniques the user will be allowed to choose the images, or icons or pictures from the set of images. It is very easy to remember and use for long time [14]. Some of the commonly used these types of passwords are PassFace, Deja Vu, Triangle, Movable Frame, Picture Password, Story, Man and Jetafida. In these types of techniques the users need to click on the images which will be having either faces or the shapes or objects like animals and so on. In certain types of passwords the users have to select the objects by continuous dragging. But these had serious problems like dictionary attacks. For example in the PassFace the users will have the tendency to choose the face which is more attractive which makes it easy for cracking. Another sub division on this type of password is Cued Recognition like we have in Story. Where the user will be creating Story is created based inter related images. In the beginning it seems to be easy, but the users sometimes not choose the passwords which in general related and found it difficult to use in long run [14].

Based on the Biometric technologies for authentication we have Keystroke dynamics. It is a process of analyzing the way a user types at a terminal by monitoring the keyboard in order to identify the users based on habitual typing rhythm patterns [15]. There are widely many keystroke dynamics are used Static at login, Periodic dynamic, Continuous dynamic, Keyword-specific, Application-specific and so on. Likewise Keystroke dynamics in our proposed system we would like to propose a new behavior dynamics which will be exhibited by the user when dragging the images to the required position. Similarly there is mouse dynamics which will be used to analyze the behavior of the mouse called mouse dynamics. Very specifically we would like to capture the behavior of drag and drop by the user and we would like to name it as Drag Stroke.

Basic idea is that each and everyone has some time difference to recognize the image and the time taken for them to drag from one place and drop it in another place will also differ. Based on this only we would like to device the new biometrics Drag Stroke. Here we would like to use this drag stroke during the time of the login. We will be displaying the images and then the user has to drag and place the images are the particular position. The time interval for each and every drag is calculated alternatively. And if it is found similar to the value in database we will allow the user to login.

Motivation: There are some common characteristics which every graphical based password is having problem with. Some of them are stated in the paper "A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms" are as follows.

- Users were fascinated by the pictures which drawn by other users so frequently we can see the common picture for password.
- The users can hardly remember the sequence of drawing after period of time.
- Not all the users are familiar with using mouse as a drawing input device for graphical password.
- The users tend to select the weak passwords which can cause the password to be guessable or predictable and vulnerable to dictionary attacks.

For designing the successful image based password it should not be vulnerable to dictionary attacks and then it should be easy to remember. For this reasons we would like to allow the users to upload the image whichever he like so that he can set the password easily and can remember without any problem. The users will have good knowledge about the personal images over the general images which are available in the internet and also these images will be very difficult to attack. But in some case users feel that their images will be stolen so there is a need to have the random images from the internet also.

At the same time our image based system will be using the new concept on drag biometrics which will be using Drag action of mouse dynamics. Where it should have some factors like Uniqueness, Collectability Permanence and so on. The Dragstroke which we design should be in such a way it will be very unique for each and every user for the images he used to position. Then there should not be any special device as we have in the biometric systems like fingerprint, eyes biometrics. So capturing the mouse movement time for positioning will be best way to do it.

JIGSPASSZLE: Our Proposed Scheme: JIGSPASSZLE is a novel authentication system which is based on JIGSAW Puzzle Solving method. In our proposed system the user needs to form the password by selecting the parts of the picture he needs to use. Here he needs to sort the order of the parts of the image. Here the parts of the images are used for creating the password, so we would like to call them as Passimages. He should remember the order in which he selects the Passimages and has to position them in the grid according to the One Time PIN (OTP) which appears on the screen during login.

Registration is a onetime process. It mainly has three stages and each have sub stages:

- Uploading the Image
- Selecting the order of Passimages
- Verifying Passimages selection

Uploading the Image: This is the first stage during the registration of the JIGSPASSZLE system. For the security reason in our system we are not having the default images for setting the password so we allow the users to upload the images which are familiar to them. The main reason for asking the user to upload the image is to avoid attacks by search bots. After Image is uploaded by the user we will be conforming about using it for password. If the user is fine with this image we will be moving to the next stage. After finishing the uploading for the image the next stage is performed in the server side itself. In the server side the image which is uploaded by the user will be automatically divided into smaller parts which are referred as Passimages here. We have decided to have number of Passimages as 9, because having large number of smaller Passimages may confuse the user in the longer time. These 9 passimages are formed as follows. The server will take the whole image and it will form the 3X3 grid which is of equal size. Then the images are sliced and 9 Passimages are obtained. Here for the purpose of example we have used the Customized android image, created by us. But the user is allowed to use his personal images.

Fig. 1: The image Uploaded by user.

Fig. 2: Several parts of Uploaded image which made as Passimage.

The above image is uploaded by the user to set his/her password. The image is the modified version of the android doll. These are some of the example of the private image which is customized by the user itself. Other examples are own image, or family photos. After uploading the images the next process is to slice them to Passimages.

When we look at the image closer we can see that the each and every part of the Passimage is have some detailed shapes which can help the user to identify the easily at the same time it will be useful when computer automated bots search. Because of complexity in the image they take time to find what the image is. Here the passimage are shown in the order as have sliced, but it is not necessary to show in order. It is automatically randomized.

Selecting the Order of Passimages: After uploading the Passimages the next step is to select the order in which the user is willing to have which will be used for positioning them during One Time PIN (OTP) stage. We would first like to request the user to select at least of 4 images. But in our proposed system we are going to use at least 4 digit numbers to 6 digit number. Here we are randomly generating number between 1111 and 999999. There is very specific reason for this. Because in some case there are lot of attacks like shoulder surfing, Phishing attacks and so on. With this dynamic nature the user may need to position either 4 or 5 or 6 of the images he has ordered. So the attacker can get confused until he creates some system to capture all the 6 images.

Here the above images show the Passimages selected by the user from the 9 Passimages. Here he had chosen the parts of the image 5, 2,9,1,6 and 3. The numbers are derived as starting from top left to bottom right. This is the 6 images he should use whenever he wants to login. The order should be remembered and it should not be changed during the login. The images are easy to remember as we can see it there are lot of difference in each and every Passimage. Such an image will help the user to remember to lot time they no stress will be there to remember the Passimages to form the password to bypass the second level of authentication.

Fig. 3: Selecting the Passimages user order

Verifying the Passimages: The next stage after selecting the Passimages is to verify whether the user can reproduce the same images he selected. During this stage we will be giving a random number between the 0000 and 999999. At that time itself the user has to position the image on the screen. When two numbers are same like 6976, then we need to just overlap the images one above another. This stage is specially designed to check the power the user has to remember his order of Passimages, then to give practice to the real time checking and also to capture the speed how the user can set his password. This speed is very useful since we are using the mouse dynamics.

$$\text{Total Time} = \frac{\text{Sum of the Time taken for}}{\text{Total number of Passir}} \quad (1)$$

☻ (2)

Here ☻ is the total time taken for any user to set his authentication system with the help of the Passimages and ☻ is the individual time taken for the user to drag and position the Passimage from one place to another. The number of Passimage displayed will be varying according to the number generated as PIN. i.e. if we have 1111 to 9999 we will be having 4 images, then if we have number as 11111 to 99999 we will be having 5 images and finally if we have 111111 to 999999 we will be having 6 images. So the value of n depends on the number generated as PIN. At any digit of the PIN we wont have 0 as of now.

The total time T_t will be stored separately in the database and also the individual time taken to position the image.

$$At = \frac{\text{Total time taken to place all the Passima}}{\text{Total number of Passimages whi}} \quad (3)$$

i.e. A_t = ☻ (4)

After finding the Total time and individual time to position Passimages we are in need to calculate the average time A_t. The Average time is very important to calculate because we are going to use the dynamic nature of numbers i.e. from 1111 to 999999. i.e. number of digits varies it may be 4 or 5 or 6.

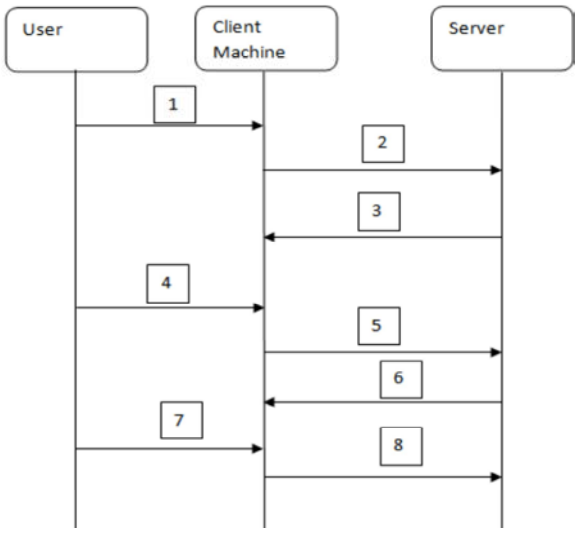

Fig. 4: User Registration

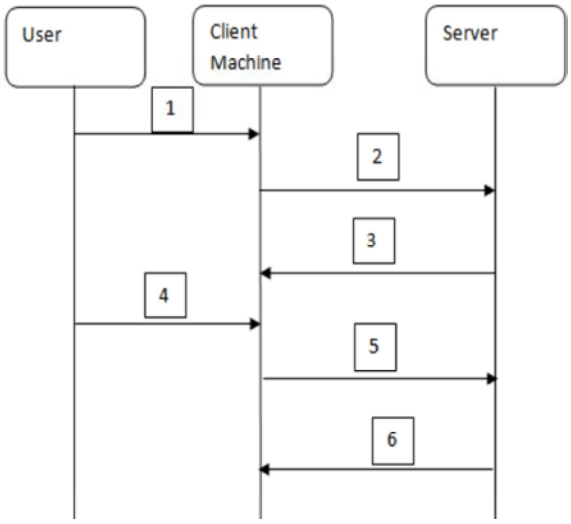

Fig. 5: User login

Whenever the user logins the system each and every time we need to find out individual times and from that we need to calculate the average time after calculating it we need to check whether with the value in the database it matches, we can allow upto 1 second difference.

Proposed System Workflow: Previously we have discussed how our proposed system is working. Here we would simplify the working procedure of the proposed system. Here both the registration process and the login process are displayed.

Registration to the System: First we would like to discuss about the registration process with the ER diagram above. For the registration process first the user will be giving his user name and password. We will be checking whether the username (e-mail ID) is already existing if not we will be accepting the user. Then they are saved in the database. After that the user is allowed to upload the image he wishes to keep as password it is displayed with the number 1 in the diagram. Then it is sent to server where the images are sliced into 9 small pieces and displayed to the user in the client machine. Then the user will select the order of the Passiamges which is the step 4 of the process. Then the order is saved in the database at the server side. After this the user is displayed with the sample One Time PIN(OTP) for checking whether he can remember the Passimages or not and at that time we were calculating the drag dynamics which is show at step 6. After this the user will enter everything and then it saved in the database which is shown at step 7 and 8 respectively.

Login Process: First the user will give his user name and the first level password which is step 1, then these username and password is forwarded to the server in the second step i.e. step 2. If the details are found correct the server will generate OTP and also randomize the order of Passimages and send to client machine to display it to the user which is step 3. The user will be position the Passimages according to the order he have and OTP which is step 4 same time the image id which is chosen is sent to the server along with time for placing it which is step 5, step 4 and step 5 is repeated continuously until he has placed required number of Passimages (either 4 or 5 or 6). Then in server the average time is found out along with the individual times, if they are found equal then the user authenticated.

Forget Password: It is not always possible to remember the password. Sometimes the human has the possibilities to forget the password. At that the system should respond properly to that. When it is a normal text based password we can normal give the user name and the password to their email id's or any other devices. But here we are using the image based authentication, so it is little bit difficult to give the images in mail. Even when we do like this the user will get confused. So we have divided the process into two parts.

Email ID to Access: In the first step of forget password the user is requested with the Email ID. He should enter the Email ID which he used during the registration process. The mechanism followed here is same as we do

for registration. First we will be checking whether the user has given email Id properly or not. Then we will check whether it is existing in our server.

Checking Text Password: Here we are concentration only on the image based password. If the user forgets the text based password we can send it to his mobile number. If the user forgets the text based password then he should do this step of verification without fail. After entering the proper email ID, he should give his text password. If both are satisfied only we can say that the user of authenticated user. Else we will give the link for his secondary email ID.

Security of JIGSPASSZLE: Here we have discussed about the various possible attacks and how secure the proposed system. The traditional attacks can be classified as: Brute Force, Key Loggers attack, Shoulder Surfing, Dictionary Attack and Social Engineering Attacks, Guessing and so on.

Social Engineering Attacks: Social Engineering attacks is the practice of obtaining the confidential information from another users by psychological manipulation of legitimate users in the. In this type of attack the attacker will just do interaction with the user and do tricks to get the sensitive information without are against the policies. Using this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes [15]. Attackers or Social engineers make the user to trust his or her words rather than using computer tools or other protocols to get the access. Our proposed system is very difficult to attack by Social engineering method. There are several reasons. First and foremost our system is purely image based password and the Passimage is generally not a whole image rather it is a part of the whole image. It is very difficult for anyone to explain the parts of the image and the order in which they have selected but it possible for anyone to remember the order of Passimages. The second main reason is that we are using mouse dynamics (i.e. Dragstroke) in combination with image based password. The time difference of each and everyone to drag and position the image defends the social engineering attack easily. Phishing Attacks is one of the examples for social engineering where the user credentials are stolen with the help of the website which will look as real website but are fake in nature. Here it is very easy to defend it with the help of dragstroke. But if the attacker captures the time he can device the machine to crack the password. But here the attackers should also know the image which is used by the user. So trying to do phishing attack is very difficult.

Brute Force: This is one of the most famous attacks in this world. Here the attacker will be trying all the maximum possibilities to crack the image. The more complex a password is, the more secure it is against brute force attacks. Usually with this attack most of the passwords are cracked easily even when the time taken for cracking the password is high. Here we are having combination from 00000 to 99999 making it total of 100000. Trying this many combinations takes very long time. First we are having 9 passimages and then have to choose which 5 images will make the one time password. Then we have to order them which are ordered by the user. Crossing this many levels makes this password very difficult to crack. And also in our system we have used Dragstroke. Cracking the Dragstroke is extremely difficult. In order to crack the password we should study the behavior or the target human very well and then design the system which can replicate very well the action of the human. But as of now implementing such a complex system is very difficult so for Brute Force attacks our proposed system can react very well and our system is very difficult to break.

Key Loggers Attack: Key Loggers are the devices or a piece of software which is used to capture the keys pressed from the keyboard and save them in text format and transfer them to remote attackers. These are mainly targeted for the gaining the credentials like passwords of the bank accounts, email ID's and so on. The key logger attacks are one of the easiest attacks done by the attacker to get the information. These are most dangerous attacks done. Many users are not aware of these Key loggers. Actually these key loggers run in the background without disturbing any one or there are hardware's which are attached with the CPU's in public internet centers. Such Key loggers can capture the text from the keyboards but it is difficult to capture the drag of the images from any position. Designing software which can find the drag movement is really very difficult and also the data needed to be transmitted is very hard. So the key loggers cannot attack our proposed system.

Shoulder Surfing: Shoulder Surfing is an alternative tricking name of "spying" in which the attacker spies the user's movements to get his/her password the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed [17]. There are two

ways in the Shoulder surfing, one way is that the attacker will be watching by himself and in another way the attacker will capture the movements of the user with the help video camera or spyware software. The attacker can closely watch the passimage order which is used by the user. But there are chances to get confusion because of Onetime password. And at the same time since there is mouse dynamics in our proposed system it is difficult to crack.

Guessing: It is one form of brute force attack, but here the attacker will have some knowledge about the user. Here the attacker will be close friends sometimes or some know person. They will try to break the authentication with the knowledge about you. These type of attacks works properly when they have the passwords which are much related to them like birthdays, names of close person and so on. Guessing will work on our proposed system when the user uses the family group photo and gives priority to the close person in that family. But they will be caught with the mouse dynamics. It is bit difficult to replicate the time the user use to drag and drop the image at the position.

Dictionary Attack: A dictionary attack is a technique for defeating authentication by finding the password from large set of data. In contrast to a brute force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities that are most likely to succeed, typically derived from a list of words in a dictionary. [17] Our proposed system mainly is accepting the images from the user, most of the people except a few have a tendency not to share their images in the internet. But since here we are going to use only for the password they will share with us. So those images will not be available in any other place in the internet. And so to form the original image it is difficult for the computer bots and sometimes for humans also without the knowledge about the images.

User Study: We conducted a study on our proposed system for a group of 10 students who has the age group between 17 and 22 who are basically undergraduate students. We made a study on how they would like to upload their original pictures or private pictures, then on willingness to use this password and the time taken to form the password.

Fig. 6: Graph showing willingness of user to use private image

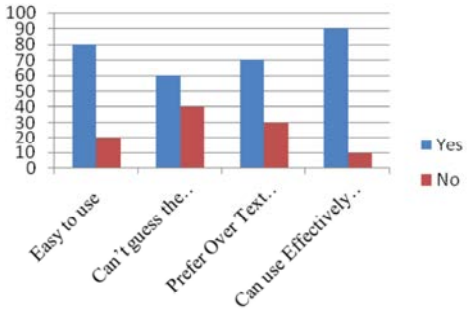

Fig. 7: Graph showing Passimage effectiveness

Usage of Picture: We asked our friends (or undergraduate students) about their willingness to share their private family pictures of any online website. Since they are young adults or teenagers 70% (7 Out of 10) of them told that they are willing to share and when we informed about our proposed system they told they are willing to have their family picture which is mostly not available anywhere in social media sites. They told us clearly that such family photo will be helpful for them to remember easily and choosing the order will be easy which will be basically based on members they like. But 30% of students told they are not willing to share their photos the main reason is that they don't want to lose their privacy and at the same time feel that giving their family photo for the passwords will be harmful because there are chances that the system administrator can misuse the picture for any other purpose. But maximum result finally showed that using family photo will be very useful for this proposed password system.

Strength of Proposed Passimages: On our survey people found that the password is very easy to use and many are willing to prefer it rather than text based password. Many stated the reason that this system look as if they are playing the game and interesting to set the Passimage in a short time. We found out gamified approach replacing

existing system and in future this proposed system can work well. Many told that this system is very easy to use and by practice they can use it effectively but some stated that old people will find it difficult when we compare with the text password, because in our proposed system we need to finish our authentication in short time and also low eye sighted people may feel difficult in using this. Some stated that in this system when they use their family photo they give preference to their close ones this can be guessed by their friends which may lead to social engineering attacks. But we suggested that the time may differ for positioning the Passimage and they accepted it when they tried, so there will not be any issue.

Average Time of Passimage Authentication: We asked 5 of our users who accepted to use their private image to our proposed authentication system. We found that it normally takes 3 to 4 seconds for them to find their private images while for other it is little bit higher 6 to 7 seconds in a average. We asked one user to first have his private image and gave the copy of that to other for 5 minutes to see. The own user is allowed to create password for him and at the same time all other also allowed to create. We found there is really a great difference in average time at least more than 2 seconds when we use our own image when compared with other images. And we had another test where we allowed other users to watch the password set the owner and asked to replicate the same to others. For that some too extremely long time where the average time difference was greater than 3-4 seconds which our system does not allow consider it as a fake user and authentication fails[12].

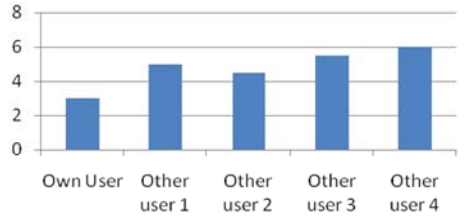

Fig. 8: Graph showing Average Time taken to set password with other images

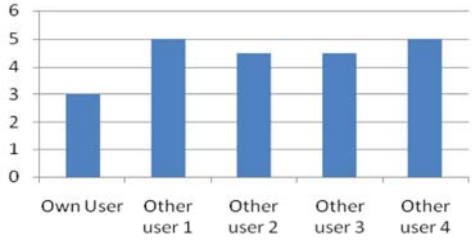

Fig. 9: Graph showing Average Time to set other users password

With the above statistics we learned that our system should have average time difference of less than 1 second and should strongly insist user to use their private images instead of other images to enter the authentication faster.

Comparative Study: We then had some study about our proposed system with the other various existing system. Right from single level of authentication to three level authentications, usage of text based authentication to sound based authentication and then finally the need for mouse dynamics.

One of the survey paper titled "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication" say combinations of passwords listed password system is strong than passwords with one factor.

- Conventional + Keystrokes Dynamics
- Conventional + Click Patterns
- Biometrics + Conventional + Keystrokes
- Conventional + Memorable

Keeping in mind we have designed our password system where the user can Memory it easily, behavior based and Dragstroke. We feel this combination is stronger than any system which was previously available. Here we would like to share some of the previous works and their drawbacks and how our system works well.

Level of Authentication Systems: For long time the authentication systems were using only single level authentication system. We had lot of advantages users will be selecting strong passwords, it is effective in network, administration had the good ability to manage users and their configuration, overhead caused during resetting the passwords is reduced when compared to multilevel authentication and provided users with the convenience of having to remember only a single set of credentials and it reduces the time taken by users to log into multiple applications and platforms. Then due to various attacks like man-in-middle, social engineering, phishing and keystroke loggers top companies introduced multi level authentication. Google introduced two step authentication first where after giving the user name and password successfully we need to enter the PIN which we receive in our mobile phones. These are widely used but had some little drawbacks, like the user is always in need to depend on another device or other services in the web and it consumed lot of time as user has to wait sometimes due to network failures these second level authentication

PIN's took long time to receive. Some system used multiple authentication system which will have two factors like password and the biometrics behavior like keystrokes. These multiple factor authentications are very difficult to break as it had biometrics of a person [13].

In our system we have used multiple factor authentication which includes image recognition, remembering the order and drag behavior of a person. We also proposed it as the second level of the authentication, where in the first level normal user name and password is given and in second we will introduce our system. In our proposed system we have suggested a new way to avoid dependencies of mobiles in such PIN. Whenever the user logins he will get auto generated PIN which will be used to position the images in the order he has chosen. We will be showing this PIN in the user screen itself, it won't be harmful, since the user need to drag and position the images and not to enter the PIN. Such systems are new currently no other authentication system has used it and also our combination clearly is perfectly strong.

So in short our System is designed with Memorable + Recallable + Biometric + Image based +PIN generated, System.

Methods of Authentication Systems: We have different methods of authentication like text based, sound based and image based. Sound based authentication is recently trending and it has been developed a year ago and now Google is trying to integrate with its Android based smart phones for its login. The sound based login is the second level of authentication and in this high frequency sound is sent to the mobile phone of the users. Here the high frequency sound is sent to the mobile and then the mobile should be placed near the computer where the user is going to login. The sound signals are encrypted and contains data of the user and other details.

Traditionally text based passwords are used. They have lot of problems and attacks. Text based password is easiest authentication but faced several different problems like easy brute force attacks, Phishing attack, social engineering, key loggers and so on. The computation in this type of passwords is very easy and the users need to remember his password to login. For more security many companies started using second level authentication which had One Time PINS(OTP). They are usually sent to mobile phones and then user needs to type them in the screen using keyboard. In both the system they have trouble with having mobile all the time with them. Our system has no dependencies like this[14].

Ours proposed system is purely an image based system, where the user will need to remember the order he needs to use. Here the user need not have special hardware with him like mobile phones for logins, here the OTPs will be available in the screen itself. Our system will not face many difficulties faced by text based system and comparatively the bandwidth used for the password is higher than text based but it is lesser than sound based password system. Our system is combination of many factors so it is stronger than any other existing systems.

Different Image Based Authentication Systems: We here would like to compare different Image based authentication which are available previously and which are discussed Graphical Passwords: A Survey by Xiaoyuan Suo, Ying Zhu G. and Scott. Owen. We have compared each and every graphical password system surveyed by them and they have divided them as Token based authentication, Biometric based authentication and Knowledge based authentication. We have not differentiated them and took them as a whole and compared our proposed system with the existing system. After this survey we have told how our system varies with these existing system and how our is secured than others.

The above table descried varies existing system and its drawbacks. When compared with our proposed system we came with some conclusion. It is very easy to identify different parts in an image and we can easily remember it. Most of the image based authentication fails due to brute force attacks and dictionary attack but in our system both the attacks are not possible because we are going to use the private image instead of images available in the internet and also we are going to use Dragstroke which is based on the drag behavior of each and every person. At the same time the amount of data passed to the server should be less, in our system we are passing the ID's of the image in the order after collecting everything at the same time we are sending the time taken for position them. In almost all the image based authentication we have same amount of data to be carried. And the time that will be taken to pass our whole authentication system will be between 12-18 seconds which is acceptable time for image based system [15-16].

Table 1: Comparision of various image based authetication system

Proposed Technique	Usability Authentication Process	Memorize ability	Possible attacks and difficulties
Dhamija and Perrig based on visualization	The user first need to pre select certain number of images and during the time of authentication he need to select same to pass the authentication	It is very easy to memory images by the user as they see it with their eyes.	Shoulder suffering and Brute Force
Sobrado and Birget	Here the user needs to click on the objects which are available in the screen, there will be 1000 objects.	Crowded with many objects, they can find the object with little difficulty	For people with problems in eyes it will be very difficult to use. Brute force and shoulder suffer attacks works perfectly
Man, et al.	User needs to select number of pictures from Pass-objects. User needs to type the position of the pass-objects.	User needs to remember alphanumeric code	Faces all the problems faced by text based passwords. Using key loggers we can capture everything easily.
Passface	Users are allowed to choose 4 faces which they like and can remember easily. During authentication from the grid they need to select the face which they have selected previously.	It is very easy to remember the faces of persons.	The time for using this longer and people had the tendency to use very famous faces. Due to this behavior dictionary attacks were easy on this at the same time we can do brute force attack also.
Jansen et al.	Users need to select their favorite pictures from the grid	Remembering the scenarios are very easy.	Due to the size limitation we had the Brute force attack problem.
Jermyn, et al. and Passdoodle	Users are required to draw the secret test or diagram in 2 dimensional grids.. For authentication they need to reproduce the same drawing in the same sequence.	It is very easy to draw the image.	Dictionary attack and shoulder suffering.
Syukri, et al.	Here the users are required to give their signature in the screen for authentication.	It is easy to remember the signature	The main drawback is it is difficult to reproduce the signature with mouse. Some people can put others signature easily. So affected by Shoulder suffering.
Blonder and Passlogix	Here user needs to click on various parts of the image. Or in Passlogix the user needs to click on the various objects in the screen.	It is very easy to remember the object and the order they have clicked.	Brute force attack worked well on both.

Future Work: Currently our proposed system will be accepting the images from the user and then divides into simple Passimages for making it as an authentication system. If the user has uploaded an image with less content at some parts of the image he will find it difficult to find it and to use it. In future we can extend the image processing algorithm which can have the ability to find the whole image and understand the parts of the images, if some areas have less parts then we can resize the image so that it can be filled in whole area. Then in our proposed system we have found the total time taken for the user to position the image and also found out the average time taken for him, in future it can be extended to see how much time the users can take to position the images at the particular positions and also the number of slice for the images can be increased.

CONCLUSION

Here we have proposed a simple but effective image based authentication system which will is the combination of recall and recognition and also the uses the biometrics based on the drag of the user. This system is easy to integrate with existing web based applications. It can also be used in the e-commerce like website to authenticate the user when he tries to start the purchase of the goods and start the transactions. It is effective solution for the touch based equipments.

REFERENCES

1. Rohit Ashok Khot, Kannan Srinathan and Ponnurangam Kumaraguru, 2011.MARASIM: A Novel Jigsaw Based Authentication Scheme Using Tagging , In Proc. ACM CHI, pp: 2605-2614.
2. Anand, S., P. Jain, Nitin and R. Rastogi, 2012 . Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication In Proc of Computer Modelling and Simulation (UKSim), UK Sim 14th International Conference, pp: 547-553.
3. Nitisha Payal, Nidhi Chaudhary and Parma Nand Astya, 2012. JigCAPTCHA: An Advanced Image-BasedCAPTCHA Integrated with Jigsaw PiecePuzzle using AJAX, IJSCE. 2(5): 180-185.
4. Mori, T., R. Uda and M. Kikuchi, Proposal of Movie CAPTCHA method using Amodel Completion ,In Proc. Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium, pp: 11-18.

5. Fabian Monrose,Michael K. Reiter,Susanne Wetzel, 2002. Password hardening based on keystroke dynamics, In Proc International Journal of Information Security, 1(2): 69-83.
6. Nasir Ahmad andrea Szymkowiak and Paul A. Campbell, 2013. Keystroke dynamics in the pre-touchscreen era In Proc Front. Hum, Neurosci. doi: 10.3389/fnhum.2013.00835.
7. Adams, A. and M.A. Sasse, 1999.Users are not the enemy. Commun. ACM, 42(12): 40-46.
8. MORRIS, R. and K. THOMPSON, Password security: a case history. Commun. ACM, 22(11): 594-597.
9. Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, Jean-Pierre Seifert, 2013. SMS-Based One-Time Passwords: Attacks and Defense, In Proc 10th International Conference, DIMVA, Berlin, Germany, pp: 150-159.
10. Dhamija, R. Hash, 2000. Visualization in user authentication, In Ext. Abstracts CHI 2000, ACM Press, pp: 279-280.
11. Fabian Monrose, Aviel D. Rubin, 2000. Keystroke dynamics as a biometric for authentication,In Proc. Future Generation Computer Systems - Special issue on security on the Web archive, 16(4): 351 - 359.
12. Cranor, L. and S. Garfinkel, Security and Usability: Designing Systems that People can use. O'reilly Media, 2005.
13. Arash Habibi Lashkari, Dr. Rosli Saleh, Samaneh Farmand and Farnaz Towhidi, 2009. A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms, In Proc. Second International Conference on Computer and Electrical Engineering.
14. Farnaz Towhidi and Maslin Masrom, 2009. A Survey on Recognition-Based Graphical User Authentication Algorithms " In Proc (IJCSIS) International Journal of Computer Science and InformationSecurity, 6(2).
15. Shanmugapriya Mrs. D. and Dr. G. Padmavathi, 2009.A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges, In Proc International Journal of Computer Science and Information Security.
16. Singh Saurabh and Dr. K.V. Arya, 2011. Mouse Interaction based Authentication System by Classifying the Distance Travelled by the Mouse, In proc International Journal of Computer Applications.