Secure Authentication using Dynamic Grid pair technique and image authentication

MSc Internship
Cybersecurity

Bharath Narayanan
Student ID: X18110827

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Mr. Bharath Narayanan		
Student ID:	X18110827		
Programme:	MSc. Cybersecurity	**Year:**	2018-2019
Module:	Academic Internship		
Supervisor:	Ross Spelman		
Submission Due Date:	12th August 2019		
Project Title:	Secure Authentication using Dynamic grid pair technique and image authentication		
Word Count:	5684	**Page Count:**	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………

Date: ………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Secure Authentication using Dynamic grid pair technique and image authentication

BHARATH NARAYANAN
X18110827

Abstract

Security is key concern for any application and protecting from unauthorized user has become more challenging now a days. The enhance attacking methods have affected each authentication techniques and their architecture. The loopholes where the attacker can interrupt the security system has increased. In this proposed method a divergent technique is performed for deterrence from security breach. The novelty in the proposed method is that it is coalition of one-time secure password and image authentication test. Adding textual password and with appropriate image authentication can enhance security to the next level. The one-time secure password is generated from a grid interface provided and can be used only once and will be reformed at each login time. The one-time secure password is generated using the respective 8-character password registered. Therefore, this report discusses the vital areas of different authentication techniques to underline the gap. This report discusses the architecture of the proposed method and the implementation of how it is carried out and the evaluation of the system to distinguish the level. The proposed method can be a resistant from shoulder surfing and keylogging attacks.

1 Introduction

Security plays a key role in technology and providing a secure application is haunting task. The threat from illegitimate user can be a major threat for security and therefore a secure authentication can prevent it. Here the Authentication plays a major part and it is nothing but the one where the authorized user can access the application. Authentication guarantees the confidentiality and integrity where the proper user can get into the system or application without been interpreted by the attacker. There are many varieties of authentication being carried out and text password is the common amongst them. Even though there are various ways of authentication there will be some demerits in each of them. Day by day the cyber threats are increasing to a huge number where the attackers are motivated to gain access control of user. They try to steal the user private information without the user's knowledge causing threat to the user. The attacker uses new methods to steal the private credential. For example, installing a software without the user knowledge and running into the system as the software ceases the information. **(Rouse, 2019)**

Authentication is a process where the system identifies whether the user accessing the system is illegitimate or not. Normal type of authentication is providing user ID and password and when each time user tries to enter the respected credentials is checked whether it is matching or not. The access will be based upon the match of ID and password which is in case known as authentication factor. Authentication and authorization go together where at first the user is authenticated by the respective credentials and gives control access to the system where authorization is permission to access the files, information etc. **(Siddiqui, 2019)**

As discussed earlier there are many threats to the authentication where the hackers try different methods to steal the user credentials. The most common form of attack is sniffing of credentials where the hacker carries out brute force attack by getting the user passwords from dump sites. The other method for performing brute force attack is spraying the password. Here the hacker tries with the commonly used passwords of user and carry out in every possible way. Once the access has been granted attacker will be able to steal the private information. Shoulder surfing is another common method of attack in which the hacker gets to know the user credentials by various ways like eavesdropping. Here the attacker tries to take down the user information by looking at them or noting the text which user types. Keylogger is surveillance software or hardware tool which is used by perpetrator to thieve the private data without the user awareness. The hardware keylogger is not installed in the system as its can be connected via USB where the private credentials can be stored without the user knowledge. Whereas software keyloggers can be installed in the system and at each time when user types anything it will be stored without the knowledge which can be used for stealing the information and data. **(C and K, 2019)**

The textual passwords have been widely used for authentication purpose which can be cracked easily by the hackers. Usually users tend to use lengthy passwords which is very difficult to remember and due to that small passwords are used which can be guessed by the attacker easily. As the technology rises the use of biometrics authentication came into existence. It consists of using fingerprints, facial recognition etc. **(Thakka, 2019).** These authentication methods are expensive to implement and carry out. To fill the gap in this proposed research the user will be able create small password and at the same time it ensures more security. In the deployed research will have two-way dynamic authentication in which user have to undergo. If any one of the authentications is failed, the user will not be granted access. The maximum length of password which the user can choose is eight. One part of authentication is image and the second one is using dynamic grid interface where the user will be able to select the secret password to protect it from the hacker who can shoulder surf. The proposed research is combination of image and dynamic grid password scheme with proper encryption which safeguard from the attacker. The dynamic grid interface provides numbers and alphabets from which the user must select the intersection points which comes between the two characters from the respected password.

The paper consists of related works where the previous works have been explained and the gaps between the proposed system and the works which had been implemented. The later section of the paper is the methodology of how the research is been carried out and how it is implemented. At last the future works related to this research is explained where this project can be taken into the next level which enhance security and overcome the disadvantages in the current system.

2 Related Works

The literature review here portraits the secure authentication which guarantees the security to the application. The study provides the detailed study of different researches which is like the proposed research. There are many researches based on the secure authentication which uses cued click points and graphical authentication. The cued click points are nothing but one in which the user must choose cued click points at the time of password creation and when at the time of login, they must correctly remember the cued points which has been selected. The major disadvantage of this authentication method is that it's time consuming and user must recollect the exact points which in case is challenging. In textual passwords, more the length it is difficult to remember the password. To overcome that only limited number of passwords is granted for the user. The research also portraits the drawbacks of previous researches which led to implementation of this project.

2.1 Graphical Authentication

The graphical authentication plays a major role in securing the authentication feature thereby improving the efficiency and scalability. The cued click points are one amongst them where the user must select the registered click points which he/she select during the password creation **(Sonia and P.C, 2019)** stated that usability and security can be increased with the usage of hotspots which is a combination of Pass Points, Pass Faces. During the login process user should select the points in five images correctly in order to get the access. The erroneous points when clicked will be notified to the user so that they can rectify. This technique provides recall mechanism where the incorrect login will be displayed to the user. User can select images either from the hard disk or the images provided by the application. The utmost drawback of this system is that it consumes a lot of time to authenticate where the hacker can take the advantage by shoulder surfing the user's click points.

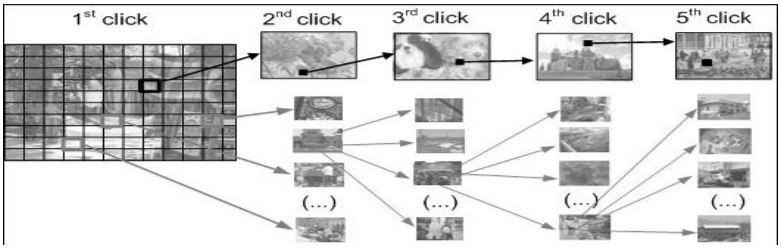


Figure 1: representation of click points **(Sonia and P.C, 2019)**

The attacker finds many ways to interrupt the user system to steal the private credentials. One such method is shoulder surfing attack where the hacker can steal the information without the knowledge of user by looking at their system. To avoid that session-based passwords are introduced **(Prabhu and Shah, 2015)** where user must undergo two-way authentication. Here it is the integration of illusion pins and images. In different order it combines the two keypads and images so that to enhance the security. The illusion pin while selecting will not be visible and it changes at every authentication which makes difficult for attacker for carrying out the shoulder surfing attack. The second authentication in the above technique is to choose the color rating which makes the user very hard to remember the exact rating.

As the technology developed more sophisticated authentication techniques came into existence. The motion images were introduced by **(Sharma, Dembla and Shekhar, 2017)** to increase the security. The password used here is video where it will be divided into frames with the help of open source computer vision tool. Advanced encryption standard is used for encrypting the frames which is extracted from the respected video. The merit of this approach is that hacker cannot break down the password easily. But the approach is very hard to carryout in real time where the login process should be extremely fast to enhance the efficiency. As a drawback, users can easily remember their images and predict the passwords easily by the cyber criminals. Story was also used from the users for their authentication process. It is also a worse process, but it is better than face recognition because users choice was less predictable. The web-based password authentication scheme can easily resolve the problem of graphical authentication. It uses single block function to resolve the problem of digital signature as well **(Tidke and Khan, 2019)**

As said earlier the major factor of security is secure authentication. The graphical authentication in order to overcome the disadvantages of textual passwords. To advance the graphical authentication cued recall recognition authentication technique was introduced **(Masrom, Towhidi and Lashkari, 2009)** The cued recall algorithm is used with the help of Pass Doodle, draw a Secret (DAS) which are the drawing method is used. At the time of registration, the user must draw a symbol and save it. At the time of authentication user must draw at the exact cell points in order to login successfully. The Syukri Algorithm is also used where the signature should be drawn by the user at the time of registration and it is checked when at the time of authentication. There were successful authentications with this technique, but the hardest part is that it cannot be used by every user as many will not be aware of how the mouse point works.

2.2 Dynamic Authentication

Instead of using pixels in image as the password which can be an easier way for perpetrator to note down. To avoid that Draw as Secret method was used where instead of image pixels the story should be chosen by user where they can draw a curve in the images of their own choice. **(Gao et al., 2010)** proposed a system in which the user is provided with the set of images at the time of registration. In the selected image user can draw a curve in one order which will be saved. At the time of login, the user should correctly draw the curve in the respected images with the same order which he/she registered. At each time of authentication, the images get refreshed and the order changes with a mixture of other images which confuses the hacker to note down the curve which the user is drawing as the pattern changes.

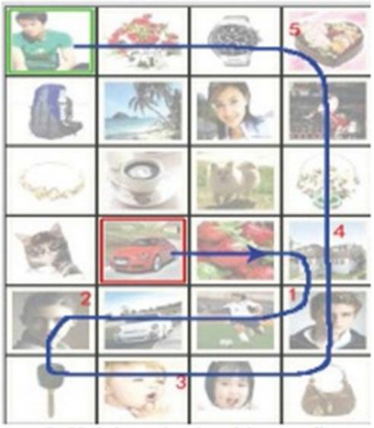


Figure 2: representation of DAS pattern **(Gao et al., 2010)**

For preventing the keylogging persuasive cued click points was used which makes a weak password strong. Using this persuasive cued click points in images will lead to more security. A graphical authentication scheme was introduced by **(Gokhale and Waghmare, 2016)** where images plays a major role in performing the authentication. At the time of registration, the user should predefine the respective image. These selected images should be remembered by the user at the time of authentication. The proposed system allows user to shuffle the images and the reallocation in order to safeguard from cyber criminals. Time consuming is the drawback of this proposed research which decreases the efficiency. In order to overwhelm the drawback in the above technique the cued click points is used in password. This proposed technique **(Ashok, 2017)** can safeguard from the attacker as it can confuse them to guess the passwords correctly. The sophisticated dynamic authentication is carried out where the single password is added with strings and 4 passwords which provides an additional security from breach. The interface provides to select the characters by using the mouse and it breaks the passwords where four different passwords and strings are added. the encryption is performed in password string. One-way data encryption is used with the concept of Nesting 93(divide and nest). The password string is partitioned into single characters and each character is integrated with the alpha numeric string. The only drawback of this authentication technique is that the selection of keys is restricted to 3 to 5.

The usage of image as password can ensure much more safety to the system. The usage of cued click points where the pixels are used require a large space. In cued click points the user must select 5 different images with one pixel in each image. The remaining pixels are not used, and these 4 pixels are wasted. To avoid the above drawback the circular tolerance in image password is introduced **(Patra et al., 2016)** where the image selected are divided into circular tolerance grids to increase the password space. In circular tolerance the r can be divided equally in a same manner. The representation for the circular tolerance is mentioned below.

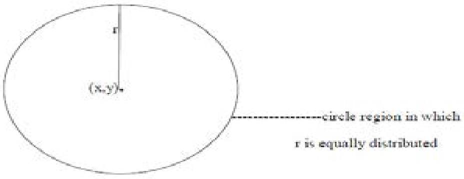


Figure 3: circular tolerance (**(Patra et al., 2016)**

The integration of textual and graphical password can enhance the security maximum which is mainly prevented from shoulder surfing attacks. Such shoulder surfing scheme S3PAS is used to combine both image and text password by **(Zhao and Li, 2007)** which can generate the login page. Each pixels or characters are transmitted one by one rather than transmitting the whole pixels or coordinates. During the login the triangle region will be displayed where the users can click the password which has been registered. The access will be granted if the user clicks the respective password in the provided triangle region. Still there are some small drawbacks in this approach which is why it is not implemented commonly. To overcome this defect the same approach can be considered with a simpler version and with more efficiency.

The use of biometrics such as fingerprints and facial scan are used to maintain the system from the cyber criminals. There are some approaches where it is a combination of both graphical authentication and biometrics. **(Singh and Bomanwar, 2015)** proposed dynamic persuasive cued click point scheme in which invisible passwords are kept foreach points. The user has the freedom to choose the password in such a way that the attacker cannot guess it. For strengthening the system time-based security is implemented and the data are encrypted. Each image which the user select has a separate view port in which the invisible password will be stored. The user must choose the exact view port to carry out to the next image or else the access will be denied. Ad1ding to that fingerprint authentication is enacted which enlarge the security level.

3 Research Methodology

The proposed method is sophisticated authentication technique where the user must undergo multi authentication in order to get into the system. This revised authentication is to overcome the challenges which are encountered in the previous techniques. This is a combination of dynamic textual grid password and image authentication with a proper encryption of saved passwords which can safeguard from the attacker in many possible ways. At first registration process will be carried out with Name, Password and email id. While registering user must select the required images from the image segment and must correctly recollect at the time of login time. After selecting the image, the dynamic textual grid box will appear which can create one-time session password using the textual password entered at the time of registration. The details about the textual grid box will be discussed in the later sections.

3.1 Standard Authentication Technique

Usually authentication is either carried out by graphical password or textual based password in which the user registers with name Id and password. The password which the user is typing is more vulnerable as it will be encountered by cyber criminals to snatch the credentials. In normal technique user first must register and remember the password (Graphical or textual) which he/she entered. If it is image password user must select the exact images or the cued click points of the images which is selected. Whereas in the textual password, the user should type the required text which they are considering as the security. These normal passwords are more vulnerable to the attacks like shoulder surfing, brute force attack etc where the attacker takes the full advantage over the system. The attacks can also occur in the database where the user private credentials are stored. The attacks like privilege abuse, denial of services, SQL injection can happen if the credentials are not encrypted properly.

The previous standard technique was based on the image and colour rating authentication. During the registration phase user create his/her ID and password adding to that should give the rating for colours from the interface which is displayed. The interface is provided with 10 colours and the rating from 1-8. User can give the rating of their own which should be remembered. Session password is created each time when user is trying to login based on the registered rating of the colour. It consists of interface which have 8*8 grids where the numbers are displayed. The image cued authentication is also performed in order to enhance the security level. The crucial drawback of this system is that the colour rating is very hard to remember during the login time. **(Sreelatha et al., 2011)**

The proposed research contains the multiple authentication where it favours the user as they can remember the textual password rather than rating the colour. This textual password is used to create one-time session password which changes each time of login.

3.2 Proposed Method

There are THREE phases carried out in this proposed model and those phases are Registering, image authentication and creating session password using textual password which have registered.

1ST PHASE: REGISTRATION

- The first step is to register into the system with required details such as name, password and email id.
- The maximum characters of password are 8 so that user can remember it easily. These 8 characters are used for generating the session password.

- The password which is registered should be remembered for generating the session password.
- The password registered is stored in data base with 3DES encryption which enhance the security from attacker.
- After when registering the textual password, a set of images will be provided from where the user can select required images of choice and can be saved for login time.
- The images will be shuffled randomly each time when the user is trying to login. It is carried out to deviate the attacker.
- The total number of image selection is 3 and should be remembered correctly at the login time to pass the authentication test. The image is predominantly used in order to safeguard from bots or robots. The image reference is illustrated in implement section.

2ND PHASE: LOGIN & CREATING ONE-TIME SESSION PASSOWRD

- The above section explains clearly about the registration process. After when registration is successful the user can login in. The login page has three main steps. The user should provide the exact user id as same as the registered one. The images will be shown in a 3*3 grid manner which consists of 9 images totally.
- The next step is to select the images provided. This is the authentication test where the correctly clicked images will allow the user to create session password. Otherwise the access will be denied.
- After the image is authenticated, an interface will appear which is used to create spot session password that can access to the application or system.
- The session password is purely based on the textual password which the user creates. The maximum number of textual passwords is 8. The password limit is set to 8 so that it can avoid the recollecting issue or the remembering problem.
- A 6*6 dynamic grid interface will be provided which consists of alphabets and numeric characters.
- When the user passes the first authentication test, they must select the session password from the interface. For generating this password user must be clear about the password which is registered. As known, the password length is 8 and it will have 4 pair.
- For each pair there will be one intersection point in the grid interface and user must select that point. The intersection points depend upon the characters present in row and column. It can be number or alphabets. If any the pair is from the same row or same column the intersection point should be mentioned as '*'. The session password created will be hidden while typing to safeguard from shoulder surfing.
- The alphabets and numbers which are in interface will be shuffled each time and their order will change.

3.3 Algorithm for Secure Authentication

1: Capture the User registered credentials and save in database.

2: The user selected image from image grid and save in database.
3: Encrypt the password with 3DES conversion.
4: Check with user id stored in database and if it’s true allows for the authentication test.
5: Validate with the user selected image with the one which is stored in database (checks by username)
6: Decrypt the password when creating the one-time session password using the key and allows to create it.
7: When choosing the intersection point, checks with the SUB characters of the respected character which is stored in database. Allows to create when it is TRUE. Deny if it is FALSE.
8: The process is repeated for the next user.

4 Design Specification

To safeguard the system or application a strong authentication is required. This proposed application is an example for that where it is user friendly and allows user to create simple passwords. This respected simple password can be used to generate one-time session passwords. The design for this proposed model is explained with the help of UML diagram where it gives the detail view of system flow. As said, the three phases of this application are Registration, Authentication Test and Login. The design is user friendly and can be used easily. The user first must register the details and should pass the authentication test where it will perceive where the user is genuine or not. If the user is valid, the access is granted or else it is denied. Let’s see more detailed about the flow of application. The whole application is structured using C#. The system requirements for proposed application is discussed later. The below illustrated is flow diagram of the secure authentication system. It clearly details the application flow.

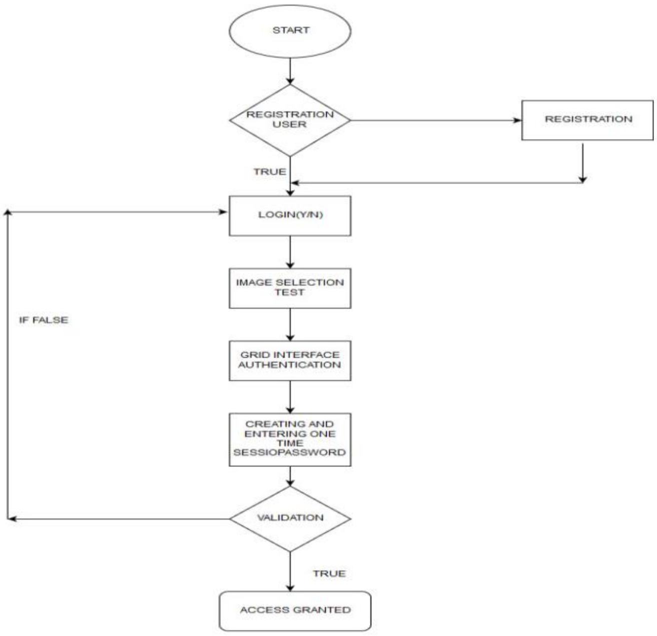


Figure 4: Flow diagram of the Application

The flowchart describe the entire flow of the system where it starts from collecting the user information like name, passoword and email id. The gathered information and credentials will be stored in database. The passowrd field will be encrypted using 3DES algorithm with a key. So that it can be used for decrptyion whle generating the one time session password. The images are to be selected for authentication test while login and the saved images will be hoarded in database. These images will be stored in a table where it check whether the user have correctly selected the respected imags from the image grid. After when registration is completed the user can login using the username and images selected. The system will only allow if the selected images are valid. The next step is to generate one-time session password which is created from the password which is registered. The Sequence diagram is illustarted below to show the accurate working of the design where it shows the workflow.

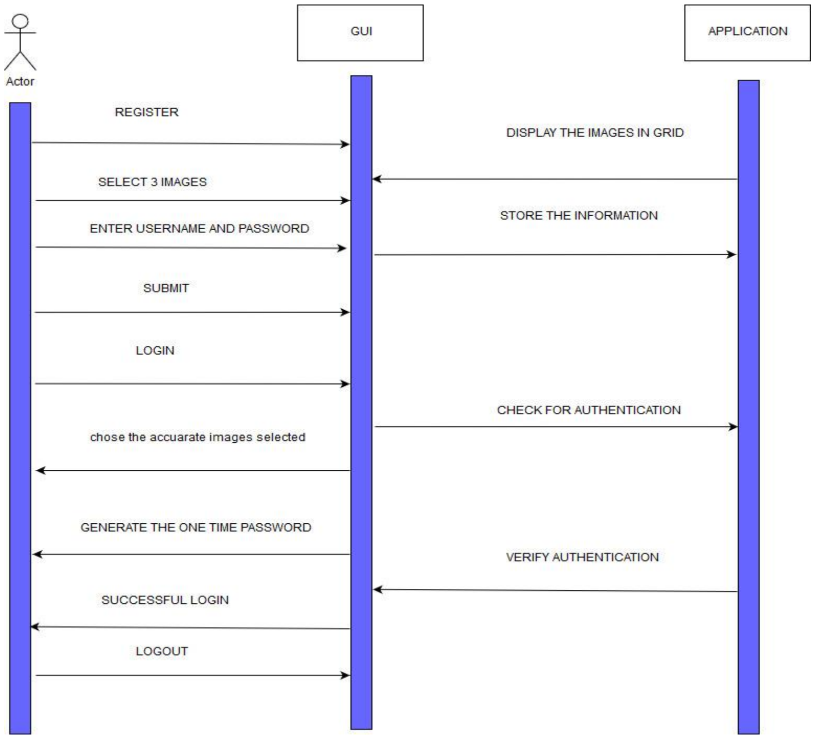


Figure 5: Sequence diagram of the authentication system

4.1 Structure of Proposed Method

The validation process will be performed after when the user selects the session time passowrd. If the validation fails the page will be redirected to the login page. The process will be repeated for the next user when they are trying to login. The structure of this application starts with the registration process and proceeding with the login process. The structure of the Design is mentioned below with a detailed diagram.

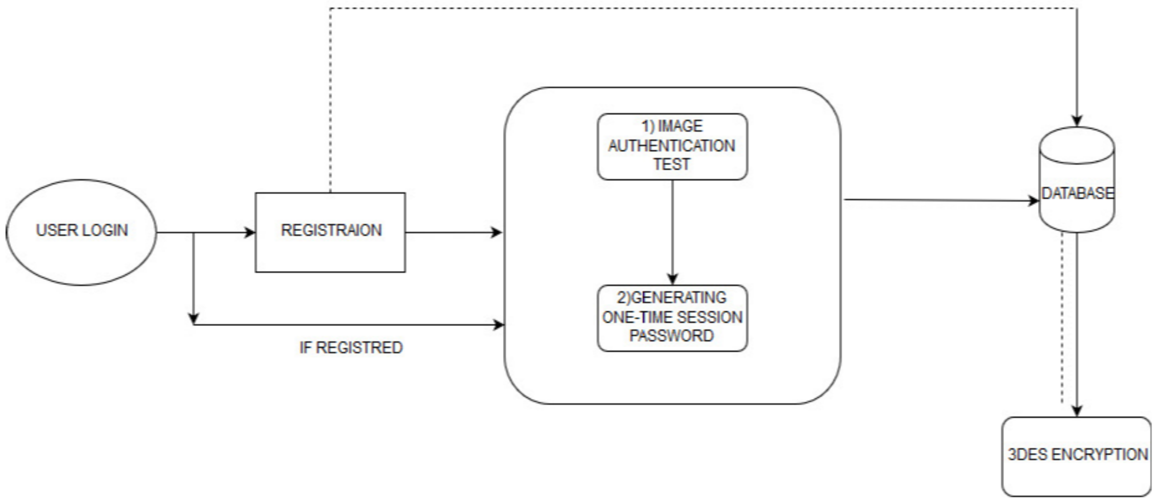
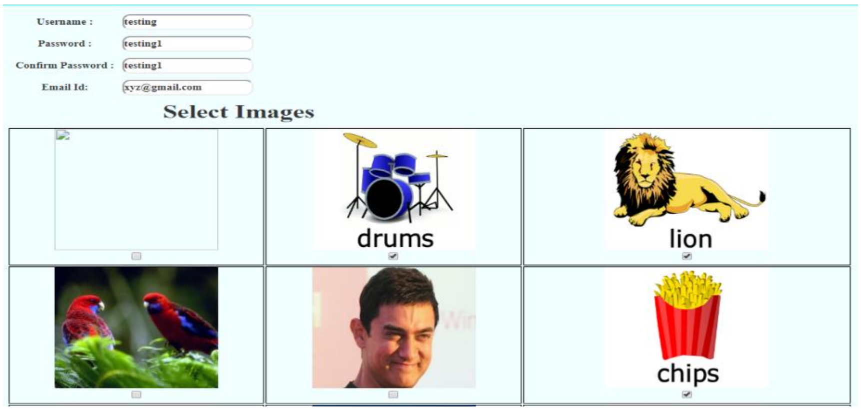

USER LOGIN
REGISTRAION
IF REGISTRED
1) IMAGE AUTHENTICATION TEST
2)GENERATING ONE-TIME SESSION PASSWORD
DATABASE
3DES ENCRYPTION

Figure 6: Structure of the Design

5. Implementation of proposed method

This section details the performance and implementation of the secure application. The first page is the registration where user can add the register the private credentials. The credentials will be stored in database which is designed by MySQL server. After registering with the details, the next step is to select images. The image grid is present which contains a set of images. The selected images will be saved in database. The system mainly has two steps, Registering and login with a one-time session password. The one-time session password will be different for each login as the characters will be shuffled.

The user will be given four fields where they must register the name, password, confirm the password and email id. After registering the personal details, the user must undergo image authentication. There will be a group of images from which the selection of mandatory 3 images are done. The registered image will be stored in database. It will be stored in a table format so that each time when user login it checks in database whether the image selected is valid or not. The length of the password is 8 and it should not exceed. This limit is set so as it will be easier for the user to remember the pair for creating the one-time password. The user registration and image selection are illustrated below.



Username : testing

Password : testing1

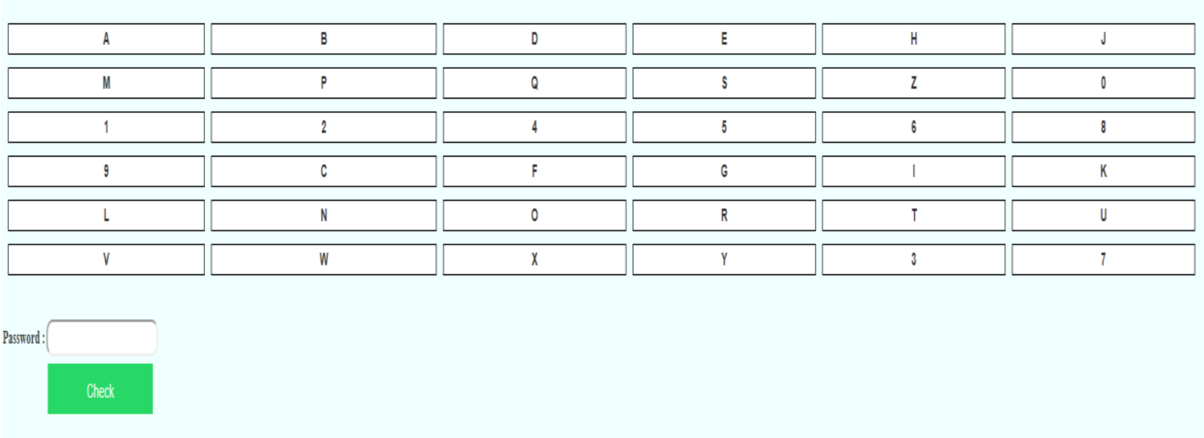
Confirm Password : testing1

Email Id: xyz@gmail.com

Select Images

Figure 7: User credentials and Image selection is being done (3 images selected)

Now the credentials are registered and required image is selected, the login will work out for the respective username. Login page have three sections which are providing the username, which is registered, choosing the preselected images and creation of one-time password. The image section will be shuffled each time of the login to test the user whether it is legitimate or not. Once the image has been selected the one-time password is creates using interface. The interface consists of combination of numbers and alphabets. The user should remember the password which has been registered. The below shown is the interface section.

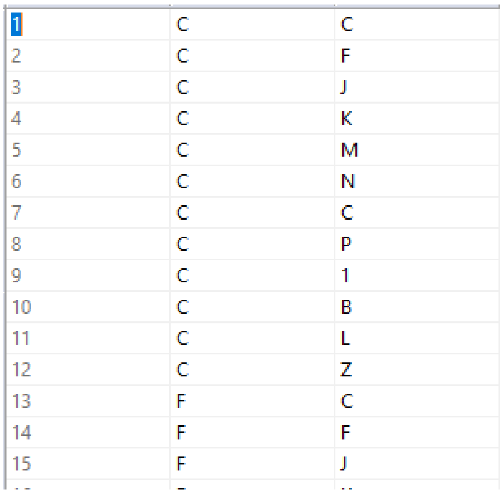


A	B	D	E	H	J
M	P	Q	S	Z	0
1	2	4	5	6	8
9	C	F	G	I	K
L	N	O	R	T	U
V	W	X	Y	3	7

Password :

Figure 8: Grid interface for secure Authentication

The password "testing1" is used for creating the secure password. The key has 8 characters and it has 4 pairs. Each pair has an intersection point in the grid box. The assembly point is selected and typed in the text box which is hidden. The two characters in the same row or column is typed as * because they have no intersection point. The login page is successful when correct points are mentioned. For logging next time new secure password must be created. The intersection point is calculated based on the sub characters. The sub characters change each time when refreshed. Sub characters will be stored in database and will be checked at the time of entering the secure password.



1	C	C
2	C	F
3	C	J
4	C	K
5	C	M
6	C	N
7	C	C
8	C	P
9	C	1
10	C	B
11	C	L
12	C	Z
13	F	C
14	F	F
15	F	J

Figure 9: Sub characters stored in data table

Once the user selects the exact crossing point the welcome page is displayed otherwise the access is denied.

Welcome:testing5

Figure 10: Access page with correct secure one-time password

6 Evaluation

To check the performance of the proposed method with the alternatives the results are compared and are noted down. The proposed method provided accurate results comparing to the previous one. The previous approach was using the colour rating which the user takes time for registering and or login time. This is because of the remembrance issue. Here in this approach as the textual password is of 8-character limit the user can remember it easily for generating the one-time session password.

6.1 Registration Test

The first test was conducted using 5 usernames and checked the time for registration using image and textual password. The average time for the 5 users is illustrated in tables. The login time using the session password is calculated separately.

Registration Method	Average(seconds)	Maximum Time(sec)	Minimum Time(sec)
Registering the textual password	38	35	42.5
Registering the Image for authentication test	49	45	53
Total Average for Registration- 43.5			

Table 1: illustration of time for registration (5 users)

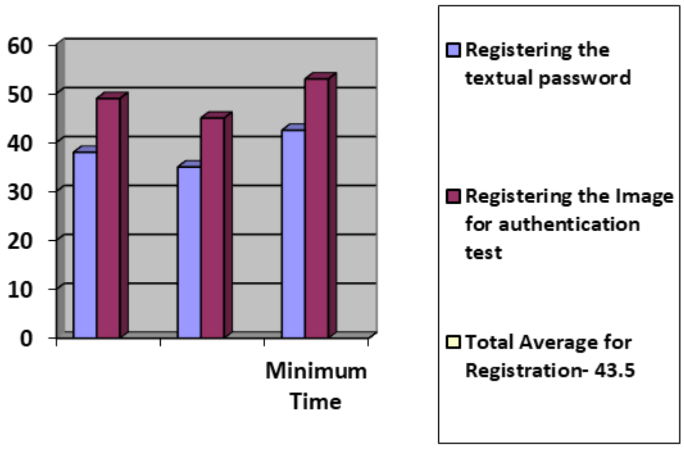


Figure 11: Graph representing the table

6.2 Login Test (for one-time secure password generation & authentication test)

The above results show that the 5 users can register with textual and image authentication without wasting the time. Now the login time was checked for two phases. First phase is to recollect the images selected at the time of registration and other one is the login time using one-time password with the textual password given by the user. The time is based on the user remembrance of the image and textual password (8 characters).

Login Method	Average(sec)	Maximum Time	Minimum Time
Image Recollection	17.5	20	15
Generating one-time password	49	52	46
Total Average for Login time- 34			

Table 2: illustration of Login time (5 users)

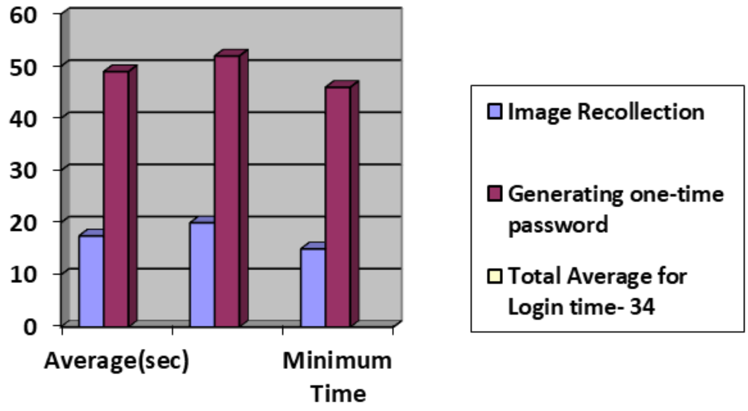
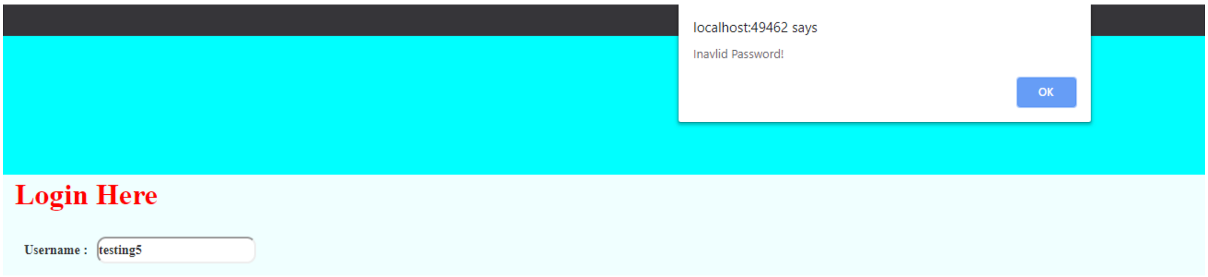


Figure 12: graphical representation of Login time (5 users)

The above result portraits that the 5 users who registered were able to remember the image and textual password. The image authentication test was approved at the first attempt by majority of the users. The textual password was remembered easily by the users as the characters was 8. The one-time secure password was generated easily by maximum users except one or two as the technique was bit difficult to understand. The time taken would be less comparing the previous results as the textual passwords are easy to recollect rather than the colour rating authentication.

6.3 System Security Check

The system was checked based on security factor. It is checked whether the system allows only legitimate users and not the suspicious one. The legitimate users are one which have followed correct steps during the registration and login with appropriate details. It is also tested whether the improper secure password is allowing the access. The system is also not allowing when the user fail the authentication test.


localhost:49462 says

Inavlid Password!

Login Here

Username : testing5

Figure 13: invalid password popping up when improper secure password is entered

6.4 Discussion

The registration and login time test were conducted to check whether the proposed system provide accuracy and it is reliable than the previous approach. In previous technique the user must rate the colour and remember the rating for each colour which will be a challenging task at the time of authentication. Here the 5 users were registered, allowed to login and the test was successful. The registration and login were done efficiently. As said this method have two approaches, one is the registration using textual and image authentication. The users were able to carry out the image selection in an efficient manner. The second phase is login using image recollection (authentication test) and the interface grid where the one-time secure password is generated. The users were able to recollect the images during login time as the images will not fade out from the brain and it is easy for remembrance. The image authentication test will decide the user can create the secure password as if the test fails even though when user creates the one-time password it will be denied. The users were able to create the one-time session password with the registered textual password. The textual passwords were easy to recollect as there are only 8 characters in the password. The problem is that user find it difficult to create the secure password from the interface. Some repeated 2 times to create the secure password. This can be modified by providing a precise interface. This can be even prolonged by allowing user to create password more than 8 characters to increase security much more. But overall the proposed method is an efficient method for secure authentication and can be used to enhance the security to the system.

7 Conclusion and Future Work

Preventing day to day cyber-attack is a challenging task. For this securing the authentication will be one of the countermeasures. This sophisticated method is performed to prevent from shoulder surfing, brute force attack and keyloggers. Various researches have been studied to implement the method. This method is an integration of dynamic grid interface and image authentication to generate one-time session password. At the registration time user can create limited textual password and can select images for authentication test. During login time the selected images can be used for test. The secure password can be generated from the character grid box from where the user should intersection point of the registered password which has 4 pairs. The authentication will be denied if the wrong points are entered.

The proposed method can be enhanced by allowing user to set the textual password more than 8 characters which can be sometimes a threat for the attack. The registration can be also used with one-time secure password where it will enlarge the security. Instead of mandatory image selection for authentication test, a different efficient method can be used to save the time and to reduce the space. The interface grid can be made much simpler and can add the all the characters using alphanumeric as here only numbers and alphabets should be used.

References

Rouse, M. (2019). *What is Authentication? - Definition from WhatIs.com*. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/definition/authentication [Accessed 27 Jul. 2019].

Siddiqui, A. (2019). *Authentication vs Authorization*. [online] Medium. Available at: https://medium.com/datadriveninvestor/authentication-vs-authorization-716fea914d55 [Accessed 27 Jul. 2019].

C, S. and K, S. (2019). Hypervisor based Mitigation Technique for Keylogger Spyware Attacks.

Thakka, D. (2019). *Advantages and Disadvantages of Biometric Identification*. [online] Bayometric. Available at: https://www.bayometric.com/advantages-disadvantages-biometric-identification/ [Accessed 29 Aug. 2019].

Sonia, C. and P.C, v. (2019). Graphical Password Authentication Using Cued Click Points. *ESORICS 2007*.

Prabhu, S. and Shah, V. (2015). Authentication Using Session Based Passwords. *Procedia Computer Science*, 45, pp.460-464.

Sharma, A., Dembla, D. and Shekhar (2017). Implementation of advanced authentication system using opencv by capturing motion images. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*.

Tidke, S. and Khan, N. (2019). Password Authentication Using Text and Colors. *www.ijsret.org278International Journal of Scientific Research Engineering & Technology (IJSRET)*, 4(3), p.278.

Masrom, M., Towhidi, F. and Lashkari, A. (2009). Pure and cued recall-based graphical user authentication. *2009 International Conference on Application of Information and Communication Technologies*.

Gao, H., Ren, Z., Chang, X., Liu, X. and Aickelin, U. (2010). A New Graphical Password Scheme Resistant to Shoulder-Surfing. *2010 International Conference on Cyberworlds*.

Gokhale, M. and Waghmare, V. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *Procedia Computer Science*, 79, pp.490-498.

Ashok, P. (2017). Dynamic Cryptographic Algorithm to Provide Password Authentication using Cued Click Points. *International Journal of Informatics and Communication Technology (IJ-ICT)*, 6(2), p.123.

Patra, K., Nemade, B., Mishra, D. and Satapathy, P. (2016). Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features. *Procedia Computer Science*, 79, pp.561-568.

Zhao, H. and Li, X. (2007). S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*.

Singh, N. and Bomanwar, N. (2015). Improved Authentication scheme using password enabled Persuasive Cued Click Points. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*.

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. and Manoj Kumar, V. (2011). Authentication Schemes for Session Passwords Using Color and Images. *International Journal of Network Security & Its Applications*, 3(3), pp.111-119.