IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

Three Level Graphical Password Authentication System with File Encryption

Sushma Y S[1] and Prabhudeva S[2]
Student, Department of Computer Applications[1]
Professor & Director, Department of Computer Application[2]
Jawaharlal Nehru New College of Engineering, Shimoga, Karnataka, India
sushmagowda55555@gmail.com and prabhudev@jnnce.ac.in

Abstract: *One of the major problems in today's word is security. Security threats can be seen everywhere in the whole world. From the beginning we just use single level authentication but it is not giving much security. To provide more security, Three Level Graphical Password Authentication System (TLGPAS) used. This is the more secure idea to implement three level password authentications for real users. Usually, textual password is generally used for authentication and password is one of the most used techniques to recognize all computers and other communication devices. The process of graphical password is choosing images then come in to the textual characters. In image password, user have to use the image for password. Clicking in different places on image user set password. Picture password there - first user have to select an image in jpg format to use as a password and then user can set the password by clicking on the image in different places. We generally know that graphical password is not easy to predict and it is quite difficult.*

Keywords: Text based password, Graphical password authentication, Click point tolerance.

I. INTRODUCTION

Authentication password provides huge security for user. There are so many authentications password system can be seen in everywhere. But so many passwords authentication can be easily broken. we commonly used one method for user identify in computers and other communication devices by Password. In this project three level password authentication are used.

This project consists of three logins along with three different kind of system password. As long as level of authentication increasing the difficulty of password also increases. If user want successfully login they must give or input password correctly. User can set any type of password by their choice. Many users use shortest password which is easy to remember that, also those passwords can easily guess so hacking chances are more.

The process of graphical password is choosing an image rather than textual format. manually easy to process graphical information and large volume of storage. In generally huge characters of password or alphanumeric passwords are very difficult to remember rather than recognizing the pictures on different kind of persons, places and things.

II. LITERATURE SURVAY

1. Fawaz A Alsulaiman et al [1], the author proposed a 3D level graphical password schema. simple text-based password, 3-dimensional password, biometric, 3dimensional virtual environment, graphical password is used here. 3D password is large number of passwords. In 3D password user do not have to provide their figure print.
2. Shipra Kumari et al., [2] the authors defines that this paper is based on remote based authentication system. here we used 3D geometry with the biometric values are used here. Biometric values are used for security purposes. Because body parts characteristic cannot be copied.
3. Khazima Irfan et el., [3] the author defines that the project is textual based graphical authentication password it is used for shoulder suffering observe. the large-scale dictionary is traditional based text password. In graphical password we can used both text based and image based graphical authentication password. And it is also implemented on result of android Applications.
4. Ming Jiang et el., [4] In this paper we can see the graphical password in two ways by the mobile user authentication. In this paper author explain that the how this generation peoples use mobile devices trustworthy.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

In smart phones we can set password in different format like pattern password, textual password, 4-digit common password and the biometric. the above paper is 2-way password and it if knowledge based. Web and Android are the 2 different demos are used here.

5. Deepika Gupta et el., [5] In this paper we can see the graphical and textual based authentication of combination are used here. It is virtual environment schemes. Graphical password contains less space taken then the textual password. Textual password contains the number of characteristics and sequence of alpha-numeric symbols. Password is in uniquely appears.
6. M Hamza Zaki et el., [6] In this project based on key the password is authenticate. In this project password is secured. In text-based password had hacking chances are more. Because any one can easily analyse. In the above scheme password provides more security like digits, keys and pattens. In patten format user can recognise in the form of maps, keys and dumpy digits. If the user want to login they firstly recall the given pattern and text password mapping. This is easy to recall for humans and it provides more security from attacks.
7. Salah Refish et el., [7] In this paper author use PAC [Password Authentication Code]. It is main issue in more applications such as websites and data base systems. In this password authentication are confirmed by the user. They used one method called routing in message passing networks [RMPN]. It gives the correct bit position to reach destination. By using RMPN method it gives security for both online and offline hack. This method had advantages such as it gives privacy for password and key sessions.

III. PROPOSED METHODOLOGY

In proposed system, we can set graphical password by system design. System design has a many steps to set. The graphical password used to file encryption and then file decryption.
In graphical authentication has a high secure password. Because it is in image password.
The proposed system must follow the below mentioned steps are

1. Registration Phase.
2. Login Phase.

3.1 Registration Phase

In the Registration Time, User first set the username. After that user was creating the password by choosing a random picture that type of password is called graphical password. User has to choose images. User can choose minimum of 3 or maximum of 5 images. After choosing images, the next step is click tolerance. Click tolerance is size of boxes. Lesser tolerance defines the small click points; larger tolerance is defining the big click points. The workflow of this registration phase is as shown in figure1, below:

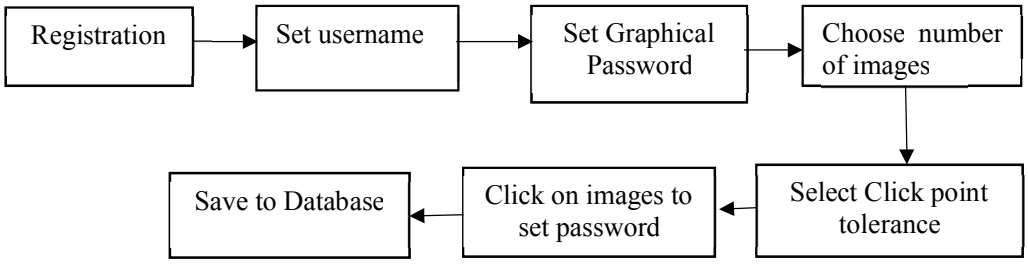

Figure 1: Work order steps in registration process

After setting an tolerance, over the images, boxes will be displayed. If the user does not satisfy the current location on images, they can change the box location by shuffle button option. On each image, there are 3 click pointers and after each click on images and corresponding click tolerances, all are stored in the database. These all steps are in the registration phase.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

3.2 Login Phase:

In the login Phase, the first step is entering username. The user must enter username correctly. If the user does not give correct username, we cannot move to the next step. It shows that username is not found. If user enter the correct username, then we can move to the next step. By the next step, system displays images. those images are we set in the registration phase. Over these images, we click the exact location that the we set location at the registration phase. By clicking on images at correct location, it processes the next step. If the clicked location is wrong, it does not process the next step.

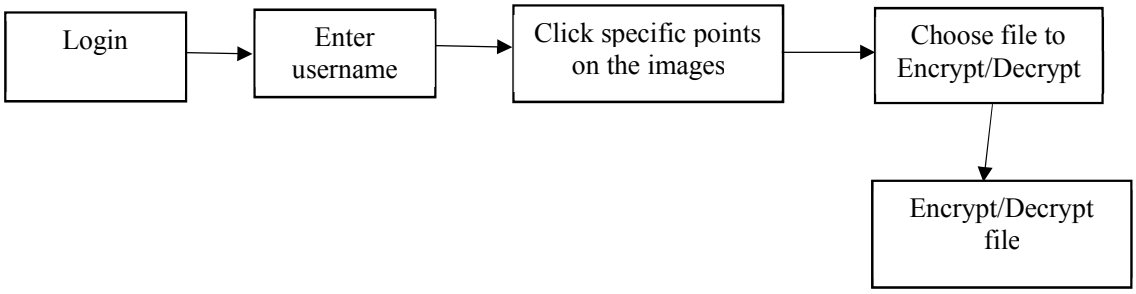

Figure 2: Login phase steps

After we click all the correct locations on images, User passing the Graphical Password Authentication. The system displays the User Interface window for encrypting the files. By this user interface window user can encrypt the files or decrypt the files.

IV. RESULT ANALYSIS

In this section, we see that user must register before the login process. In Registration process conatins four fields : First name, Last name, User name and Email ID. The following snaph shots highlights the login and user data entry processing steps (see figure 3).

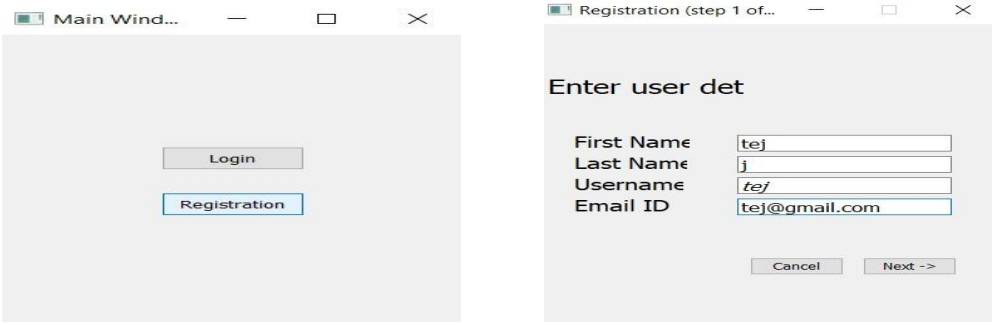

Fig 3: Registration process and upload user data.

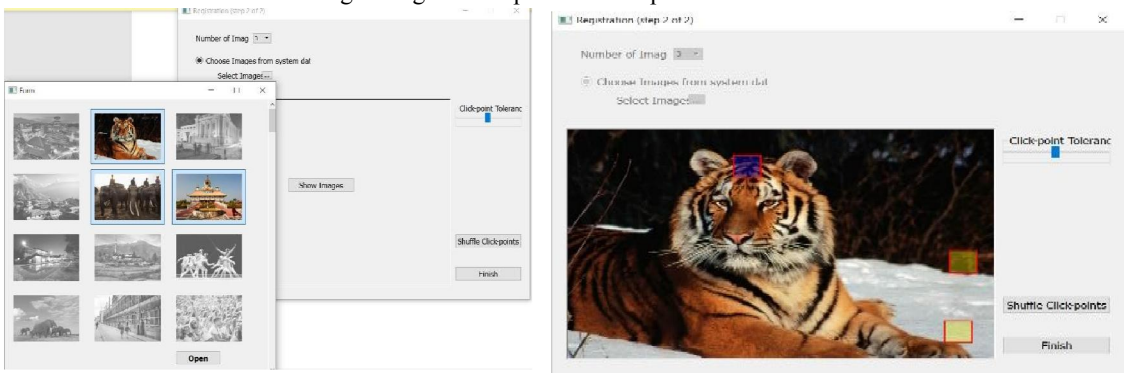

Fig 4: Successfully complete register process.

After filling complete user data, it shows the user added successfully notification. Which means user successfully added their data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

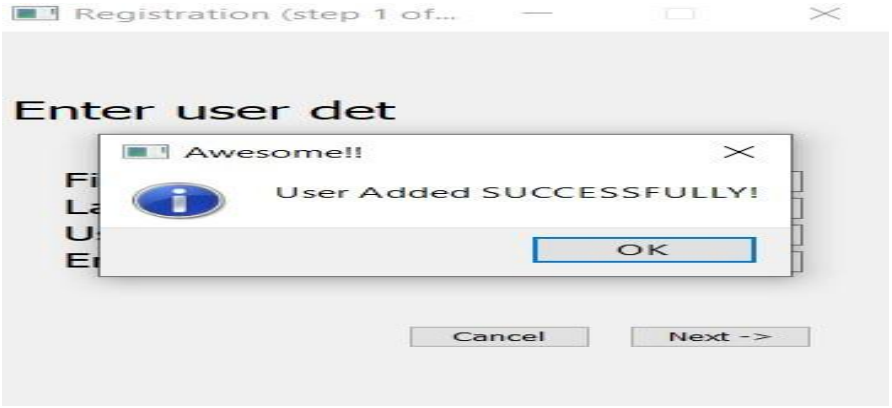

Fig 5: Set Graphical password by choosing images and Click tolerance.

After successfully register user set a graphical password. By selecting an images, user can set password. User can select minimum of 3 images and maximum of 5 images. After selecting images, user do tolerance. Tolerance means size of pointer or box. If tolerance is less, the size of click box is smaller. If the tolerance is more, the size of click box is bigger. And we can shuffle the click pointers also, by using Shuffle click pointers.

Fig 6: Login process

After the completion of registration process and set the Graphical authentication password by choosing an images, know user move to login process.

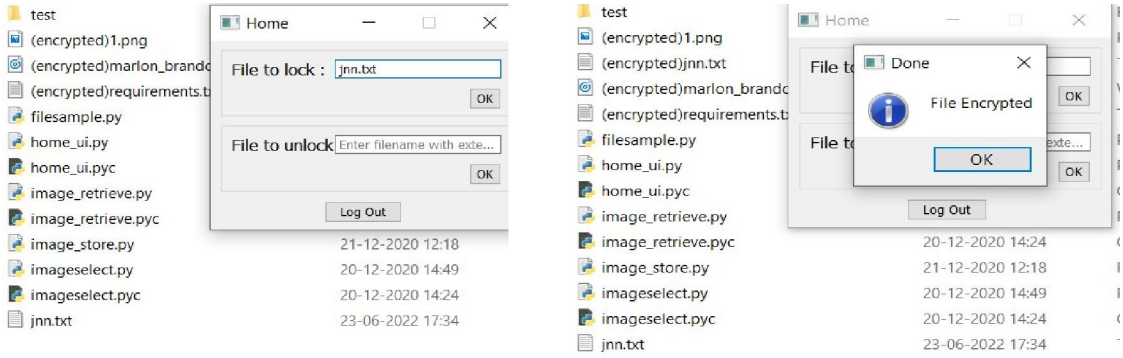

Fig 7: lock the existing files.

After login process, user lock their existing file. User enter the file name in front of file to lock syntax. That file is locked and deleted at the existing place. And the file is encrypted.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

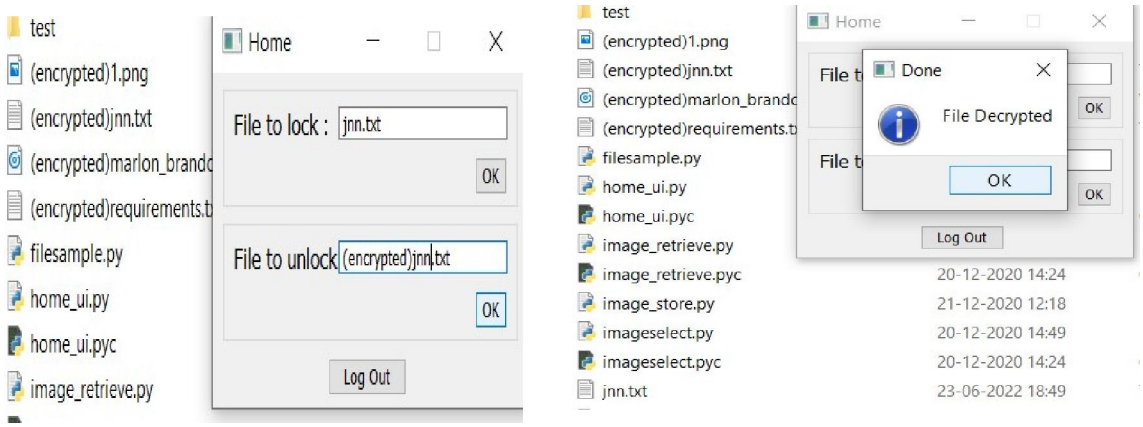

Fig 8: unlock and decrypt the file

Once the file is locked and the file is encrypted by the user. user can recover the file by unlock the file and files are decrypted. When user enter the encrypt file name in the File to Unlock field. The locked files is automatically unlock and files are decrypted the previous position.

V. CONCLUSION

Graphical password authentication system provides a huge security rather than the other authentication technique. The graphical password used for file encryption and file decryption process. Graphical authentication is high security password because it is in image password. The process of graphical password is choosing an image rather than textual format. Manually easy to process graphical information and large volume of storage. In generally huge characters of password or alphanumeric passwords are very difficult to remember rather than recognizing the pictures on different kind of persons, places and things.

REFERENCES

[1]. Fawaz A Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema", Multimedia Communications Research Laboratory University of Ottawa, Ottawa, Canada [fawaz, abed] @mcrlab.uottawa.ca.

[2]. Shipra Kumari, Hari Om, "Remote Login Password authentication Scheme based on Cuboid Using Biometric", Department of Computer Science and Engineering Indian School of Mines, Dhanbad. shiprakumari18jan@gmail.com, hariom4india@gmail.com

[3]. Khazima Irfan , Agha Anas , Sidra Malik , Saneeha Amir, "Text based Graphical Password System to Obscure Shoulder Surfing" ,Department of Computer Science COMSATS Institute of Information Technology Islamabad Pakistan khazima_irfan@yahoo.com ,aghaanas.007@gmail.com ,sidraa.malik@gmail.com ,saneeha.nust@gmail.com.

[4]. Ming Jiang, Ai He Connected Finance Lab Suning R&D Center Palo Alto, CA, USA {ming.jiang, ai.he}@ussuning.com Kuangyu Wang, Zhengyi Le Connected Finance Lab Suning R&D Center Palo Alto, CA, USA {kuangyu. wang, zhengyi.le}@ussuning.com." Twoway Graphic Password for Mobile User Authentication".

[5]. Deepika Gupta Computer Science deepika.gupta1218@gmail.com, Dr. Vishal Goar Computer Science goar.vishal@gmail.com, Akhand Singh Computer Science akhand.mca2009@gmail.com Shikha Mathur Computer Science shikhamathur806@gmail.com." COMBINATION OF TEXTUAL AND GRAPHICAL BASED AUTHENTICATION SCHEME THROUGH VIRTUAL ENVIRONMENT".

[6]. M Hamza Zaki, Adil Husain, M Sarosh Umar, Muneeb H Khan. "Secure Pattern-Key Based Password Authentication Scheme". Department of Computer Engineering Aligarh Muslim University Aligarh, India.

[7]. Salah Refish, "PAC-RMPN: Password Authentication Code Based RMPN" .Dept. of Computer Engineering Imam Jaafar Alsadiq University Najaf, Iraq manatheraa@yahoo.com