International Conference on Advances in Materials, Computing and Communication Technologies
In Association withInternational Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Resist Shoulder Surfing Attack for Consumer Smart Device

Abisha S[1], Mrs. M. Maria Sheeba[2]

[1]PG Student, Department Of Computer Science and Engineering, Ponjesly College of Engineering, Tamil Nadu, India

[2]Assistant Professor, Department Of Computer Science and Engineering, Ponjesly College of Engineering, Tamil Nadu, India

ABSTRACT

User authentication is the process that is exercised millions of times around the globe by using different techniques and methods. The most prominent way of authentication is alphanumerical password forms that have been used for decades. Authorized access is becoming a challenging issue because of the introduction of modern technologies. In addition, traditional alphanumerical passwords have significant security issues, for example, humans forget the combination of keys due to the selection of a difficult key combination. Moreover, when they choose an easy key combination, this helps hackers to crack their passwords easily. Traditional passwords are also vulnerable to several types of attacks, for example, dictionary attack, brute force attack, and malware. To provide an easy and more secure authentication technique, a graphical password has been introduced in this paper for consumer electronic devices, which uses an image or a set of images for authentication. Here, categorized the existing graphical password methods into recognition based, cued-recall based, pure-recall based, and hybrid techniques. Due to the limitations of the existing graphical passwords, have introduced a new technique, named Graphical Random Authentication Technique (gRAT), which generates a randomized set of images every time a user tries to authenticate him/herself by maintaining the security and usability at the same time. The gRAT technique is also tested by user-centric evaluation in terms of security, usability, usefulness, and utility, and the experimental results show that the proposed technique is more secure and useful in the real-life authentication applications.

Index Terms: Graphical password, Authentication methods, Information security, Usability, Usefulness.

I. INTRODUCTION

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper and lower case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with Long-Term Memory (LTM) than verbal representations. Image based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image based passwords are to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities.

In this project, a secure graphical authentication system named g-RAT that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of randomized set of images every time a user. The g-RAT provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

This project elaborates on the existing graphical password techniques and reviews the potencies and pitfalls of these schemes. In addition, a novel graphical password authentication technique is proposed, which is more reliable and secure as compared to the available techniques. The key objective of this project is to find that how to design a graphical password scheme, which provides usability while maintaining user security. In other words, the main objectives of this study are to:

1) Equally focus on the usability and security characteristics.
2) Study the most promising scheme by focusing on security and usability simultaneously.
3) Propose a new graphical password technique on the basis of security and usability.
4) Evaluate the proposed framework and compare with the most promising techniques.

Attacks on Password Authentication System

There are various kinds of attacks on password authentication system which are following:

A. Common Internet Attack Methods –

Common internet attack methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as denial of service attacks, but they are used in some form or another even if they aren't mentioned by name.

B. Eavesdropping –

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way.

C. Phishing –

Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishers trick users into disclosing.

D. IP Spoofing Attacks –

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP- spoofed packets cannot be eliminated.

E. Firewall –

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

F. Intrusion Detection Systems –

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

The rest of the paper is organized as follows. In Section II describes the literature reviewing graphical password. Section III presented the proposed system model. Section IV represents the performance analysis. Section V represents the discussion about the result. Finally in Section VI conclude the paper.

II. LITERATURE SURVEY

Amin et al. [2] proposed that in order to resist unauthorized access, consumer storage devices are typically protected using a low entropy password. However, storage devices are not fully protected against an adversary because the adversary can utilize an off-line dictionary attack to find the correct password and/or run an existing algorithm for resetting the existing password. In addition, a password protected device may also be stolen or misplaced allowing an adversary to easily retrieve all the stored confidential information from a removable storage device. In order to protect the consumer's confidential information that has been stored, this paper proposes a mutual authentication and key negotiation protocol that can be used to protect the confidential information in the device. The functionality of the protocol enables the storage device to be secure against relevant security attacks. A formal security analysis using Burrows-Abadi-Needham (BAN) logic is presented to verify the presented algorithm. In addition, a performance analysis of the proposed protocol reveals a significantly reduced communication overhead compared to the relevant literature. This paper proposes a mutual authentication and key agreement protocol to provide only authorized access to confidential information stored on the device with the aid of a Registration Server (RS). A new user completes a registration procedure with RS allowing RS to deliver a link via e-mail from which the user can download and install registration software in their device which also incorporates the required secure access information relevant for only each user. In order to provide secure access to files, the user provides the necessary identity, password and biometric information. The device checks the legitimacy of the user and then negotiates a session key with RS. It is to be noted that this session key is used to encrypt the files in the storage device.

Sherratt et al. [3] proposed that the Universal Serial Bus (USB) Mass Storage Device (MSD), often termed a USB flash drive, is ubiquitously used to store important information in unencrypted binary format. This low cost consumer device is incredibly popular due to its size, large storage capacity and relatively high transfer speed. However, if the device is lost or stolen an unauthorized person can easily retrieve all the information. Therefore, it is advantageous in many applications to provide security protection so that only authorized users can access the stored information. In order to provide security protection for a USB MSD, this paper proposes a session key agreement protocol after secure user authentication. The main aim of this protocol is to establish session key negotiation through which all the information retrieved, stored and transferred to the USB MSD is encrypted. This paper not only contributes an efficient protocol, but also does not suffer from the forgery attack and the password guessing attack as compared to other protocols in the literature. This paper analyses the security of the proposed protocol through a formal analysis which proves that the information is stored confidentially and is protected offering strong resilience to relevant security attacks. The computational cost and communication cost of the proposed scheme is analyzed and compared to related work to show that the proposed scheme has an improved tradeoff for computational cost, communication cost and security.

Tari et al. [4] proposed that this paper examines the real and perceived vulnerability to shoulder-surfing of two configurations of a graphical password, Pass faces compared to non-dictionary and dictionary passwords. A laboratory experiment with 20 participants asked them to try to shoulder surf the two configurations of Pass faces (mouse versus keyboard data entry) and strong and weak passwords. Data gathered included the vulnerability of the four authentication system configurations to shoulder-surfing and study participants' perceptions concerning the same vulnerability. An analysis of these data compared the relative vulnerability of each of the four configurations to shoulder surfing and also compared study participants' real and perceived success in shoulder surfing each of the configurations. Further analysis examined the relationship between study participants' real and perceived success in shoulder surfing and determined whether there were significant differences in the vulnerability of the four authentication configurations to shoulder surfing. Finding indicate that configuring data entry for Pass faces through a keyboard is the most effective deterrent to shoulder surfing in a laboratory setting and the participants' perceptions were consistent with that result. While study participants believed that Pass faces with mouse data entry would be most vulnerable to shoulder surfing attacks, the empirical results found that strong passwords were actually more vulnerable.

Van Oorschot et al. [5] proposed that the text passwords have been widely used for user authentication, e.g., by almost all websites on the Internet. However, it is well-known that text passwords are insecure for a variety of reasons. For example, users tend to choose simple passwords in favour of memorability, making them subject to dictionary attacks; and text passwords can be stolen by malicious software (e.g., keystroke loggers) when being entered from keyboards. Phishing is another serious threat to text passwords, by which, a user could be persuaded to visit a forged website and enter their passwords. Such an attack is made possible in part due to the fact that text passwords do not allow users to authenticate a server; by design they provide only one-way user authentication, and server authentication is not a design objective of text passwords alone. We propose a two-step authentication method to strengthen text passwords by combining them with graphical passwords. In this approach, called Two-Step, users continue to use text passwords as a first step, but then must also enter a graphical password, providing the following advantages: users' current sign-in experience is largely preserved; a text password alone which is stolen (e.g., by phishing) does not compromise an account; users can be alerted if not seeing the graphical password cuing image after providing their text passwords, implicitly providing server authentication; and it can be implemented in software alone, increasing the potential for large-scale adoption on the Internet.

Weiss et al. [6] proposed that the authentication mostly relies on passwords or personal identification numbers (PINs). Therefore the average user has to remember an increasing amount of PINs and passwords. Unfortunately, humans have limited capabilities for remembering abstract alphanumeric sequences. Thus, many people either forget them or use very simple ones, which implies several security risks. In this work, a novel authentication method called Pass Shapes is presented. In this system users authenticate themselves to a computing system by drawing simple geometric shapes constructed of an arbitrary combination of eight different strokes. We argue that using such shapes will allow more complex and thus more secure authentication tokens with a lower cognitive load and higher memorability. To prove these assumptions, two user studies have been conducted. The memorability evaluation showed that the Pass Shapes concept is able to increase the memorability when users can practice the Pass Shapes several times. This effect is even increasing over time. Additionally, a prototype was implemented to conduct a usability study. The results of both studies indicate that the Pass Shapes approach is able to provide a usable and memorable authentication method.

Bicakci et al. [9] proposed that the authentication is the process to establish the identity of a communication partner. It is an essential security component of today's many internet applications. The security weaknesses of using text based passwords for user authentication are well known but most systems still rely heavily on this simple and low cost solution a recent study shows that 93 % of large businesses in UK still use passwords to authenticate users. There is a significant body of recent research exploring the feasibility of alternative approaches to provide a more secure and usable authentication solution. One promising alternative is graphical passwords. Based on studies showing that human brain is better at recalling images than text these unconventional methods aim to solve memory burden and low entropy problems of classical passwords. Among graphical password schemes click-based graphical passwords has gained popularity. In click-based graphical password schemes, users click a sequence of points on a pictorial background to create and use passwords. In-depth examination of click-based graphical passwords shows that these systems are vulnerable to predictability. Certain points (hotspots) on the pictorial background are more likely to be selected by users, which makes passwords predictable. Different attack strategies are quite successful to guess click-based graphical passwords. Some images generate more and definite hotspots than others but the hotspot problem persists even when abstract shapes or the same type of objects (such as cars, paper clips) fill the pictorial background. Pering et al. [13] proposed that the one additional risk associated with using public infrastructure is that an assailant can potentially capture all information being entered and displayed, not just data from the authentication process. For example, when users check the status of their bank accounts, they are potentially compromising both their account balance and account number. However, it is generally only necessary to display the account balance, not both. Such casual data, such as the bank account balance without the account number, could be suitably protected with a photographic-authentication scheme because it is private but not high security. A highly secure authentication technique would be overkill for such a terminal because secure authentication in itself does not guarantee the security of the data accessed. Photographic authentication aims to be “secure enough” for casual data by providing the necessary level of security without compromising ease of use. Ideally, the complete system would not even allow a user to access high security data through an untrusted terminal. In other words, just because you already showed your badge to enter work doesn’t mean you should leave your wallet on your desk. The popularity of digital photography has recently exploded because of the widespread availability of affordable consumer grade cameras and computers capable of manipulating photographs. As a result, many people have substantial personal digital photograph collections. Furthermore, as cameras become more affordable and easier to use, more people will possess large personal image collections, and digital storage capacities are rapidly increasing, providing sample space to save images. For the users who have them, these images can form a convenient authentication system that does n’t require much configuration.

Chakrabarti et al. [16] proposed that the challenge-response protocol is vulnerable to a password-guessing attack. In this kind of attack, we assume that an adversary has already built a database of possible passwords, called a dictionary. The adversary eavesdrops on the channel and records the transcript of a successful run of the protocol to learn the random challenge and response. Then the adversary selects passwords from the dictionary and tries to generate a response that matches the recorded one. If there’s a match, the adversary has successfully guessed A’s password. After every failed matching attempt, the adversary picks a different password from the dictionary and repeats the process. This non-interactive form of attack is known as the offline dictionary attack. Sometimes an adversary might try different user IDs and passwords to log in to a system. For popular Internet services like Yahoo!, the adversary can trivially choose any reasonable user ID due to the large number of registered users. An adversary can also find user IDs within interactive Web communities such as auction sites. If the system rejects the password as being incorrect for that particular user, the adversary picks a different password from the dictionary and repeats the process. This interactive form of attack is called the online dictionary attack.

Gao et al. [17] proposed that the security and usability problems inherent in text-based password schemes have resulted in the development of graphical password schemes as a possible alternative. However, most of the current graphical password schemes are vulnerable to spyware which is a program that gathers information about a computer’s use and relays that information back to a third party. To date, there have been some schemes which have made contributions to the development of graphical password in term of spyware resistance. Using a challenge-response protocol, they have an advantage in that they are resistant to replay attacks. Namely, even the third party who observes a successful login session cannot perform a replay attack. Though they have a positive effect on protecting users’ password, they are not yet sufficient to stop attackers from harvesting passwords. In this paper, CAPTCHA is used in a graphical password scheme to resist spyware. A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but are beyond the capabilities of current computer programs. CAPTCHA uses open algorithms based on hard AI problems, and has been discussed in text- based password schemes to resist dictionary attack. Innovatively, we explore CAPTCHA in the context of graphical passwords to provide better protection against spyware. As long as the underlying open AI problems are not solved, CAPTCHA is a promising way to resist spyware attack in graphical password schemes. Based on this key idea, we have proposed a new graphical password scheme using CAPTCHA, designed to be strongly resistant to spyware attack, either by purely automated software or via human participation. A preliminary user study indicates that our scheme needs to improve in terms of login time and memorability.

Liu et al. [18] proposed that the graphical passwords have been proposed as an alternative to alphanumeric passwords with their advantages in usability and security. However, most of these alternate schemes have their own disadvantages. For example, cued-recall graphical password schemes are vulnerable to shoulder-surfing and cannot prevent intersection analysis attack. A novel cued-recall graphical password scheme CBFG (Click Buttons according to Figures in Grids) is proposed in this paper. Inheriting the way of setting password in traditional cued-recall scheme, this scheme is also added the ideology of image identification. CBFG helps users tend to set their passwords more complex. Simultaneously, it has the capability against shoulder surfing attack and intersection analysis attack. Experiments illustrate that CBFG has better performance in usability, especially in security.

III. PROPOSED DESIGN

Here, propose a Pure-Recall based system for the authentication. The key features of Pure Recall-based techniques are combined in the proposed gRAT system. The layout of gRAT system is presented. The gRAT authentication method has three categories of pictures, i.e., animals, birds, and random, that users can use for password creation and saving. The proposed system is more secure, reliable, and user-friendly while maintaining the usability and security. The proposed system, gRAT, is based on the swipe-based authentication for the screen lock of consumer devices. However, gRAT uses a randomized algorithm that generates random images during the authentication process. The generation of random images helps gRAT fighting against the shoulder surfing attack better than the existing techniques. When a password is selected and learned, users should be capable to recall it every time they want to authenticate themselves. Yet users regularly forget their passwords. Due to evolving technologies and a wide variety of online accounts, users are required to remember several passwords at the same time for various accounts. These passwords likely lead users to forgetting or get confused. A password is only secure if it consists of a difficult combination of keys for attackers to guess. The password problem is defined in the current scenario where many passwords or options are available, but these are weak and-memorable or secure-but-difficult-to-remember. Thus, a graphical password is introduced as an alternative to the basic text-based password, which is easier to memorize. However, a graphical password is still not that much mature and has a number of weaknesses and prone to several attacks, for example, Dictionary attacks, Shoulder-surfing, and Phishing.

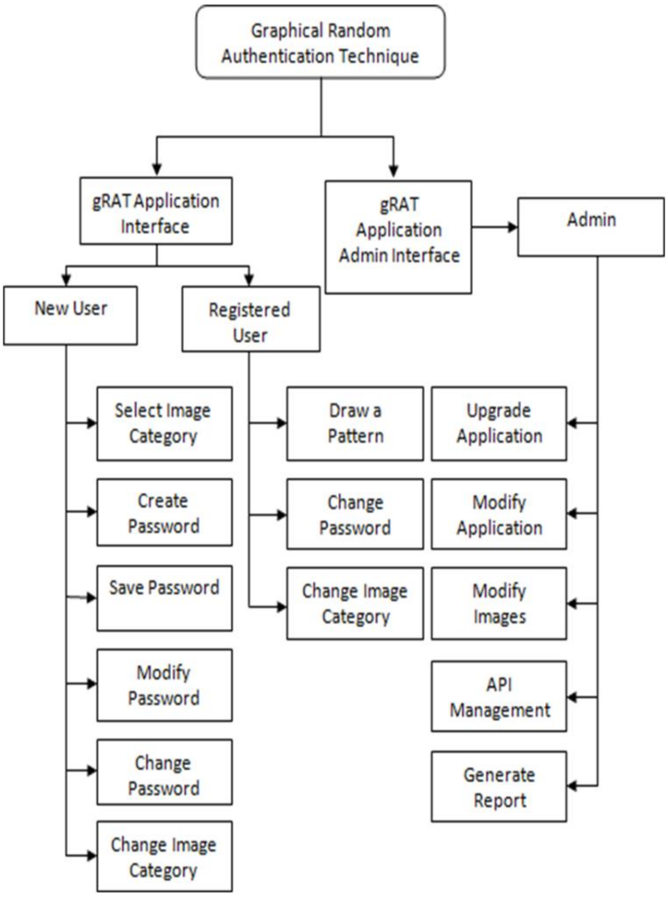


Figure 3.1 Proposed System Model

The proposed system, gRAT, is based on the swipe-based authentication for the screen lock of consumer devices. However, gRAT uses a randomized algorithm that generates random images during the authentication process. The generation of random images helps gRAT fighting against the shoulder surfing attack better than the existing techniques.

A. gRAT System Architecture

The gRAT system is a graphical password technique that uses images which are presented on the screen in a 3x3 grid. However, the highlighted part of the gRAT is that users always get a randomized set of figures. In other words, in the gRAT system the place of pictures changes every time a user wants to be authenticated. The randomized algorithm makes the gRAT resistant against the shoulder-surfing attack. The proposed system has three steps of registration and authentication. The first two steps are the registration and the last one is the authentication process, which is briefly explained below:

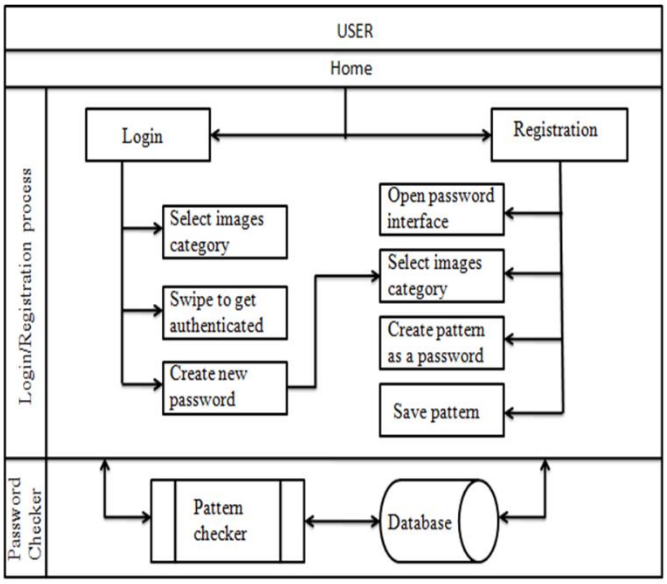
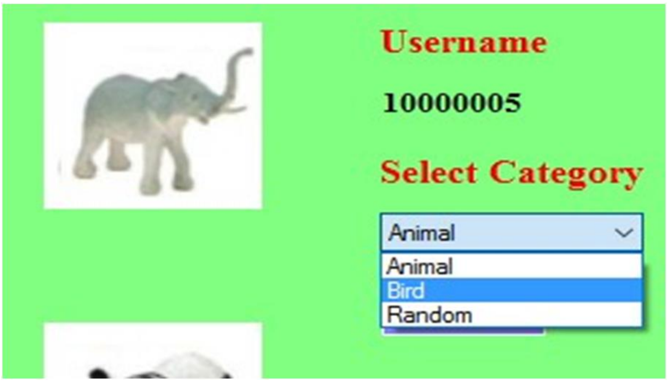


Figure 3.2 gRAT Architecture

Step 1 : In the first step, a user selects a category of images that is provided by the gRAT application

Step 2 : In the second step, the user chooses a password from a 3x3 grid picture, which is provided on the screen, and then draws a pattern by swiping on images. The password can be minimum of two and maximum of nine images. The gRAT displays the notification of "Draw a pattern to save" when the user selects a category

Step 3 : This step is about the authentication, where users draw the same pattern that has already been selected during step 2 to validate their profile. During the authentication process, a randomized set of images is presented to the users, but they need to draw the same pattern using the same set of images. The randomized set of images helps gRAT to fight against the shoulder-surfing attack. If users draw a correct pattern, then the application displays a message "correct pattern drawn", and thus they are authenticated.

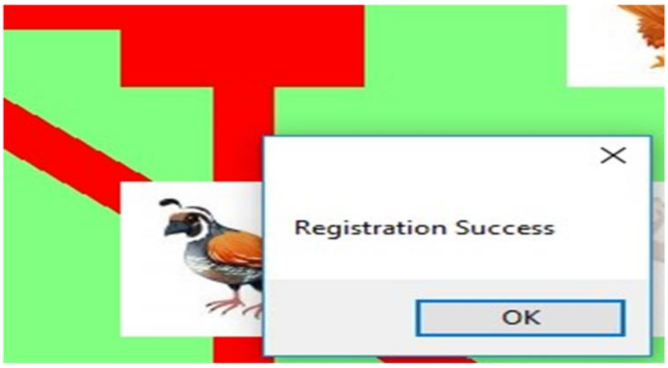


Username

10000005

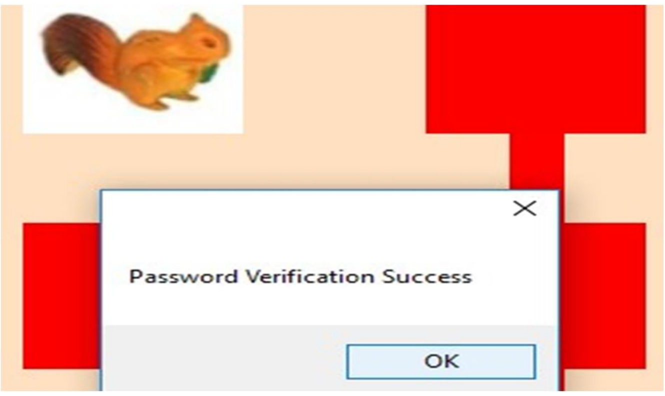
Select Category

Figure 3.3 Categories of gRAT



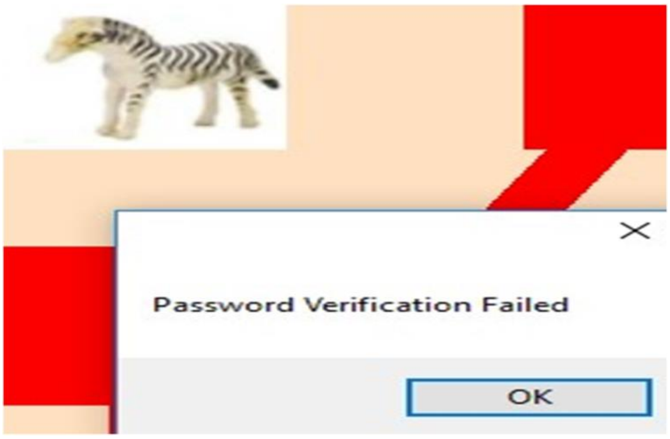
Registration Success

Figure 3.4 Password Registration



Password Verification Success

Figure 3.5 gRAT Correct Pattern Drawn



Password Verification Failed

Figure 3.6 Wrong Pattern Drawn in gRAT

In the case of a wrong pattern drawn, the user has to draw the pattern again with a randomized set of images. When the user draws a wrong pattern, the application displays a warning of the wrong pattern drawn.

B. MODULES

The proposed system gRAT is based on the swipe-based authentication for the screen lock of consumer devices. However, gRAT uses a randomized algorithm that generates random images during the authentication process. The generation of random images helps gRAT fighting against the shoulder surfing attack better than the existing techniques.

- Registration phase
- Login phase
- File management and accessing

1. Registration phase

Every system user is required to register to the system. The registration consists of a few easy steps. First, users choose the category of shapes in which they feel comfortable and then create passwords. Once the password is created, it is saved, and the same images are selected in a sequence for granting the authentication, where these shapes/images are randomized by the application during the authentication process.

2. Login phase

In the login phase, a few tasks can be performed, i.e., users can modify/change their passwords as well as change the category of shapes that they have chosen during the login phase. In the login process, authentication is granted on entering a correct password. In case a wrong password is entered, then users have several choices to enter their passwords.

3. File Management and Accessing

In file management, user can encrypt any chosen files using the encryption key for security protection. User's ends a confirmation message to server that the obtained encrypted file is correct. Next, server maintains a table against each user with the identity. In File Accessing, User makes a request to server to access the encrypted files stored in the storage database.

IV. PERFORMANCE ANALYSIS

The system evaluation is a significant stage where standard goals are considered to compare results of the proposed system with the existing ones. Explained the evaluation as a systematic method which assesses a designed scheme for its architecture, framework, and benefits. Evaluation is a major process wherein a comprehensive study, concentration, and judgment of the system lead to accurate results.

a. Time Complexity

Our implementations were single threaded with code optimization, and did take advantage of multi core capability of the test machine. Much faster image generation should viable by exploiting multi core architecture of today server and by optimizing the code.

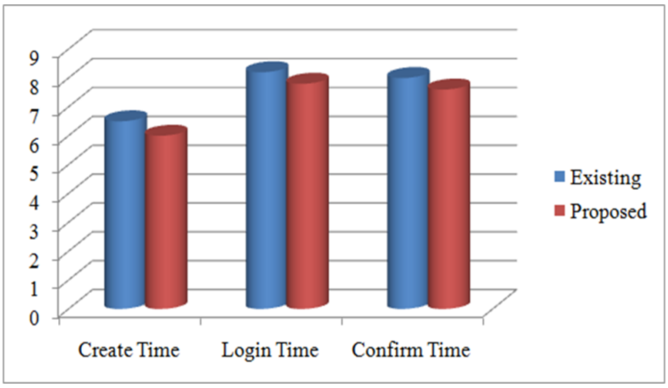


Figure 4.1 Time Complexity

This graph represents that the proposed system take less time to create or login the application, when compared to the existing system.

b. Security

The Cracking result that the passwords the participants selected for Text and proposed were reasonably strong, which match our expectation of the password complexity requirement.

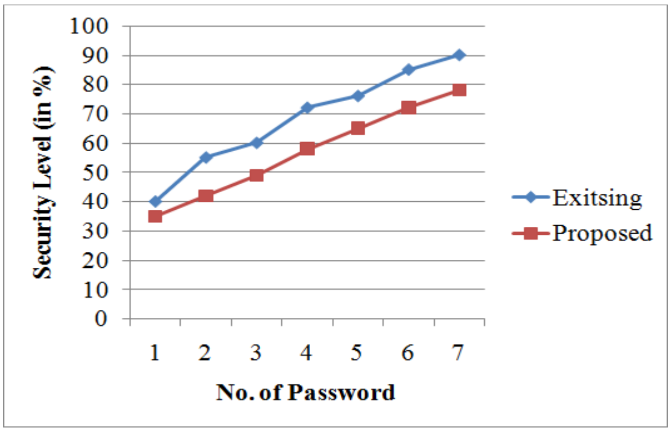


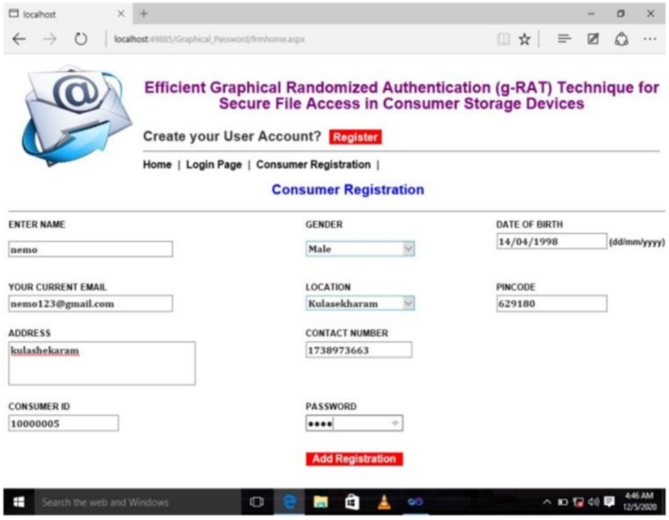
Figure 4.2 Security

The above graph represent that the proposed system is more secure than the existing system.

V. RESULTS AND DISCUSSION

The general aim of this paper is to increase the usability, security, and memorability of the graphical passwords for consumer electronic devices, thus, we focus on pure-recall based graphical passwords. We were successful at designing an innovative scheme that improves memorability as well as provides security and usability. It is deduced from the obtained results that the proposed system is more secure than the existing graphical scheme and shoulder-surfing resistant.

The following images show the result of graphical random authentication system.


localhost:49885/Graphical_Password/frmhome.aspx

Efficient Graphical Randomized Authentication (g-RAT) Technique for Secure File Access in Consumer Storage Devices

Create your User Account? Register

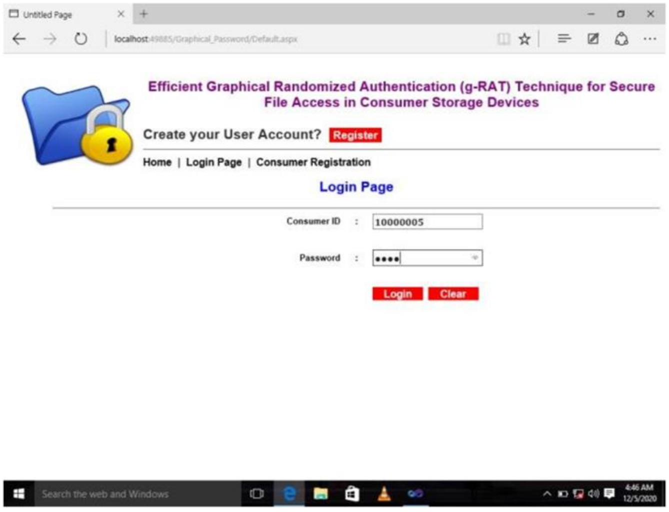
Home | Login Page | Consumer Registration |

Consumer Registration

ENTER NAME: nemo
GENDER: Male
DATE OF BIRTH: 14/04/1998 (dd/mm/yyyy)
YOUR CURRENT EMAIL: nemo123@gmail.com
LOCATION: Kulasekharam
PINCODE: 629180
ADDRESS: kulashekaram
CONTACT NUMBER: 1738973663
CONSUMER ID: 10000005
PASSWORD: ••••

Add Registration

Figure 5.1 User Registration


localhost:49885/Graphical_Password/Default.aspx

Efficient Graphical Randomized Authentication (g-RAT) Technique for Secure File Access in Consumer Storage Devices

Create your User Account? Register

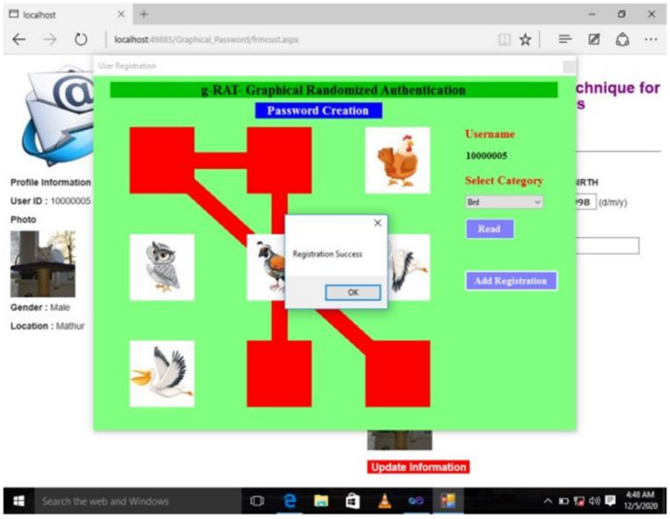
Home | Login Page | Consumer Registration

Login Page

Consumer ID : 10000005
Password : ••••

Login Clear

Figure 5.2 Login Page

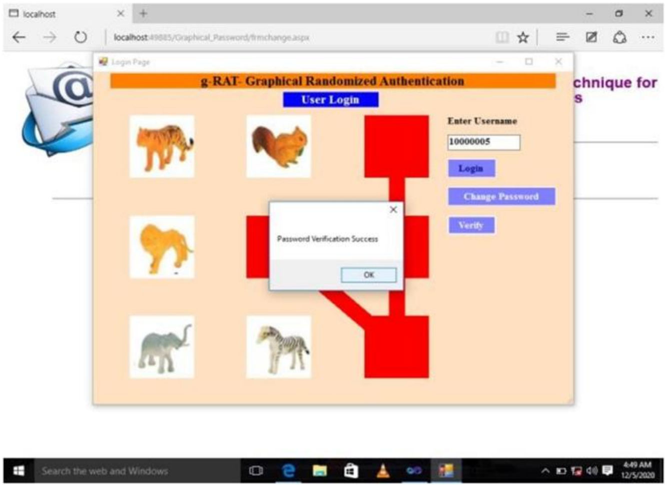

localhost
localhost:49885/Graphical_Password/frmcust.aspx
User Registration
g-RAT- Graphical Randomized Authentication
Password Creation
Read
Add Registration
OK
Update Information
Search the web and Windows
4:48 AM
12/5/2020

Username
10000005
Select Category
Brd

Registration Success

Profile Information
User ID : 10000005
Photo
Gender : Male
Location : Mathur

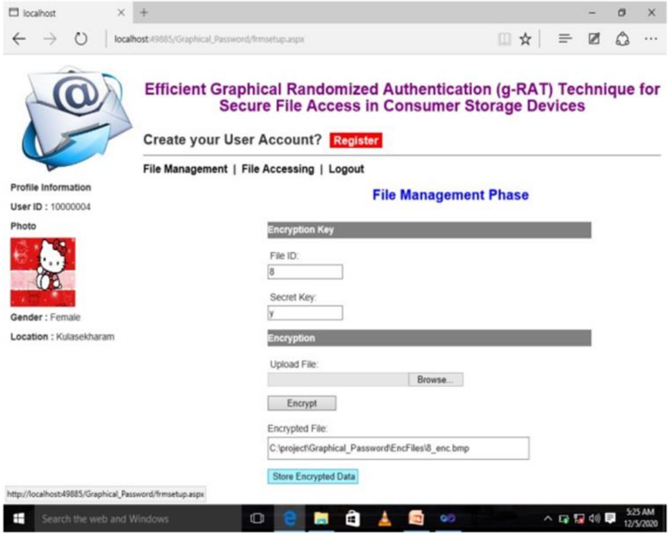
Figure 5.3 Password Registration


localhost
localhost:49885/Graphical_Password/frmchange.aspx
Login Page
g-RAT- Graphical Randomized Authentication
User Login
Login
Change Password
Verify
OK
Search the web and Windows
4:49 AM
12/5/2020

Enter Username
10000005

Password Verification Success

Figure 5.4 gRAT Login Page


localhost
localhost:49885/Graphical_Password/frmsetup.aspx
Register
File Management | File Accessing | Logout
Browse...
Encrypt
Store Encrypted Data
http://localhost:49885/Graphical_Password/frmsetup.aspx
Search the web and Windows
5:25 AM
12/5/2020

Efficient Graphical Randomized Authentication (g-RAT) Technique for Secure File Access in Consumer Storage Devices

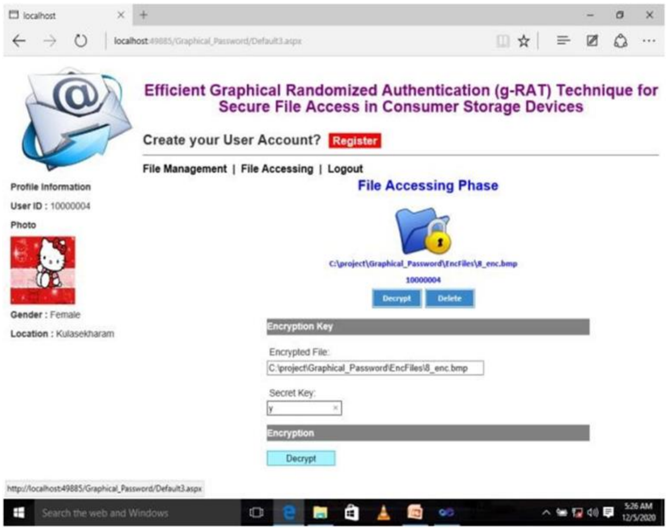
Create your User Account?

File Management Phase

Profile Information
User ID : 10000004
Photo
Gender : Female
Location : Kulasekharam

Encryption Key
File ID:
8
Secret Key:
y
Encryption
Upload File:
Encrypted File:
C:\project\Graphical_Password\EncFiles\8_enc.bmp

Figure 5.5 File Management


localhost
localhost:49885/Graphical_Password/Default3.aspx
Register
File Management | File Accessing | Logout
Decrypt
Delete
Decrypt
http://localhost:49885/Graphical_Password/Default3.aspx
Search the web and Windows
5:26 AM
12/5/2020

Efficient Graphical Randomized Authentication (g-RAT) Technique for Secure File Access in Consumer Storage Devices

Create your User Account?

File Accessing Phase

Profile Information
User ID : 10000004
Photo
Gender : Female
Location : Kulasekharam

C:\project\Graphical_Password\EncFiles\8_enc.bmp
10000004

Encryption Key
Encrypted File:
C:\project\Graphical_Password\EncFiles\8_enc.bmp
Secret Key:
y
Encryption

Figure 5.6 File Accessing

VI. CONCLUSION

The gRAT system fights against the most common attack on graphical passwords, i.e., shoulder- surfing attack, because it uses a randomized image algorithm. In the randomized image system, an observer cannot judge user's password as it generates a set of randomized pattern every time a user wants to authenticate him/herself. Finally, we examined the gRAT system through user-centric evaluation and observed that the proposed model was found more secure and useful.

VII. REFERENCES

[1]. D. Lin, N. Hilbert, C. Storer, W. Jiang, and J. Fan, "Uface: Your universal password that no one can see," Computers & Security, vol. 77, pp. 627– 641, 2018.

[2]. R. Amin, R. S. Sherratt, D. Giri, S. Islam, and M.K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," IEEE Trans. Consum. Electron., vol. 63, no. 1, pp. 53–61, 2017.

[3]. D. Giri, R. S. Sherratt, T. Maitra, and R. Amin, "Efficient biometric and Password based mutual authentication for consumer usb mass storage

devices," IEEE Trans.Consum. Electron., vol. 61, no. 4, pp. 491–499, 2015.

[4]. F. Tari, A. Ozok, and S. H. Holden, " A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. 2nd ACM symposium on Usable privacy and security, 2006, pp. 56–66.

[5]. P. C. Van Oorschot and T. Wan, "Twostep : An authentication method combining text and graphical passwords." MCETECH, vol. 2009, pp. 233–239, 2009.

[6]. R. Weiss and A. De Luca, "Passshapes : utilizing stroke based authentication to increase password memorability," in Proc. 5th ACM Nordic conf. Human-computer interaction: building bridges, 2008, pp. 383–392.

[7]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in USENIX Security Symposium, vol. 13, 2004, pp. 11–11.

[8]. R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication," in USENIX Security Symposium, vol. 9, 2000, pp. 4–4.

[9]. K. Bicakci, N. B. Atalay, M. Yuceel H. Gurbaslar,and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem," in IEEE 33rd Int. Computer Software and Applications Conf. (COMPSAC'09), vol. 2, 2009, pp. 318–323.

[10]. D. Weinshall, "Cognitive authentication schemes safe against spyware," in IEEE Symp. Security and Privacy, 2006, pp. 6–pp.

[11]. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," Int. jour. human-computer studies, vol. 63, no. 1, pp. 128–152,2005.

[12]. E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere," in Proc. 4th ACM symposium on Usable privacy and security, 2008, pp. 35–45.

[13]. T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," IEEE Pervasive Computing, vol. 2, no. 1, pp. 30– 36, 2003.

[14]. W. Jansen, S. I. Gavrila, V. Korolev, R. P. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," NIST Interagency /Internal Report (NISTIR)-7030, 2003.

[15]. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords." USENIX Association, 1999.

[16]. S. Chakrabarti and M. Singhal, " Password-based authentication: Preventing dictionary attacks," Computer, vol. 40, no. 6, 2007.

[17]. H.Gao,X.Liu,S.Wang,andR.Dai,"A new graphical passwordscheme against spyware by using captcha." in SOUPS, 2009.

[18]. X.Liu, J.Qiu, L.Ma, H.Gao,and Z.Ren,"A novel cued-recall graphical password scheme," in IEEE Sixth Int. Conf. Image and Graphics (ICIG), 2011, pp. 949–956.

[19]. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in ESORICS, vol. 7. Springer, 2007, pp. 359–374

[20]. D. Giri, R. S. Sherratt, and T. Maitra, " A novel and efficient session spanning biometric and password based three-factor authentication protocol for consumer usb mass storage devices," IEEE Trans. Consum. Electron., vol. 62, no. 3, pp. 283–291, 2016.