iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5208

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

HoneyPass: A Shoulder Surfing Resistant Graphical Authentication System using Honeypot

Arun Kumar S[1], Renu R[2], Rashika R[3], Ramya R[4]
[1]*Assistant Professor,* [2, 3, 4]*Student, Department of Computer Science and Engineering, Sapthagiri College of Engineering, India.*

Abstract: ***In today's modern world, securing the organization's data has become a major concern. To provide security, the most widely recognized authentication methods are credentials, OTP, LTP etc. These methods are more prone to Brute Force Attack, Shoulder Surfing Attack, and Dictionary Attack. Shoulder Surfing Attack (SSA) is a data theft approach used to obtain the personal identification numbers or passwords by looking over the user's shoulder or by external recording devices and video capturing devices. Since SSA occurs in a benevolent way, it goes unnoticed most of the times. It is one of the simple and easy methods for hackers to steal one's sensitive information. The hacker has to simply peek in while the user types in the password without any much effort involved. Therefore, this phenomenon is widely unknown to people all over the world. Textual passwords are a ubiquitous part of digital age. Web applications/mobile applications demand a strong password with at least one capital letter and a special letter. People tend to give easy passwords in order to remember them which can be easily shoulder surfed. To overcome this, graphical password techniques are used to provide a more secure password. In the graphical authentication system, the users click on target images from a challenge set for authentication. Various graphical systems have been proposed over the years which are shown to be more secure when compared to other authentication systems. In this paper, a shoulder surfing resistant graphical authentication system is implemented using honeypot concept.***
Keywords: Shoulder Surfing Attack, Textual Password, Graphical Authentication System, Honey Pot Concept, Data Security

I. INTRODUCTION

Security plays a vital role in any organisation. Data protection is one of the main challenges faced in any business environment. In order to protect any resources, the companies undertake various security measures. However, security has become a worldwide problem as websites have become an integral part of everyone's life [1]. The uncompromising security issues that has to be addressed in websites occur during the user authentication phase. In today's computer world, authentication is very important in order to keep the unauthorized users from accessing the protected resources. Authentication is a process that allows a device to verify the identity of a person who connects to a network resource. In order to keep the users' data private, authentication mechanism is used wherein the user types in the username and password to access their private account. However, people performing authentication process in public results in shoulder surfing attack. [2].

Shoulder Surfing attack is a direct observation approach where the shoulder surfer steals the user's Personal Identification Number (PIN), passwords by looking over his shoulder. [2,3] It commonly happens in public transports while the victim is commuting which involves a smart phone in almost all cases. A good example is shoulder surfing at ATMs, a crime in which a suspect watch over the victim's shoulder as he punches in his PIN number. The ATM screen asks for another transaction when the customers complete theirs. Some customers fail to notice the prompt and walk away leaving it on the screen. In this way, the thief enters the stolen PIN and pretends to be the user. But the phenomenon of shoulder surfing is not widely known. [4] Users tend to use the strategies such as hiding the device screen, shielding the device with their hand etc. However, by observing, one cannot get a hold with most of the victim's detailed biodata such as information about his relationships, sexual preferences, interests, hobbies, and login data. Hence, the damage shoulder surfing can cause is widely unknown. [5].

Textual password approach is used tremendously all over for authentication. During the authentication phase, websites demand strong passwords with at least six to eight characters comprising of uppercase and lowercase alphabets, numbers, and special characters. Such passwords are believed to prevent brute force attacks. [6] A password cannot be remembered if its strength is more. In [7] today's digital age, websites play a major role in one's life. People are part of an enormous amount of such websites with each containing the authentication phase where the user validates him by entering a password to access their private data. In order to remember all such passwords, the user tends to choose the same password for multiple websites which makes the password unprotected for the hackers to break. A more complex password is shoulder surfing resistant. Thus, these passwords can be easily revealed if the shoulder surfer peeks or uses video recording devices [7].

Graphical authentication systems are used in order to overcome the disadvantages of textual password systems. Here, images are used as the password instead of a string of characters. These graphical passwords are expected to be stronger and safer than textual passwords. [8] Several studies prove that a human brain has a better ability to memorize and recollect images easily when compared to a string of characters. Since it is easy to recollect the password, the user need not choose the same password for multiple websites. It makes it hard for the assailants to break the password if the user prefers to use a strong graphical password. This, in turn, increases the security level during the authentication phase. A strong graphical authentication system not only safeguards the password from brute force and dictionary attacks, but also from shoulder surfing attacks. Since shoulder surfing can create damage to the user during authentication, a strong graphical password is preferred over a textual password according to the studies conducted [9, 10].

II. OVERVIEW OF AUTHENTICATION SCHEMES

Password-based authentication schemes have been most commonly used on many smart devices when compared to other authentication schemes. The lower complexities in implementation, computation, processing requirements and so forth have led to the use of a password-based authentication system. Again, text-based passwords are more commonly used when compared to other existing authentication systems. However, various vulnerabilities were discovered by several cryptanalysts in text-based systems like brute force attack, guessing attack, dictionary attack, social engineering attack etc. In smart phones, the tiny screen size imposes some more constraints such as limited password length, implementation of easier authentication systems to increase performance etc. Moreover, the small on-screen keyboard makes typing inefficient and less precise. Consequently, the users tend to use a smaller password which makes it even more vulnerable. Since the size of smart devices is getting smaller and smaller; few authentication systems cannot be implemented in it due to its size [11].

The invention of graphical password authentication systems was triggered by the well-known limitations of textual password authentication systems. The graphical authentication systems have been generally categorized into draw metrics, loci-metrics, and search metrics systems. In draw metrics-based systems, the users will have to recall and reproduce the predefined pattern on a canvas to use the system. In loci-metrics-based systems, the users will have to recall and select the previously defined points in an image in order to log in to the system. In search metrics-based systems, the users will have to choose the predefined target images from the displayed challenge set. During the login phase, the system throws in with entirely the same images or with a few different images which were displayed to the user during the registration phase. The selection of correct target images will let the user access the system. Shoulder surfing has always been a problem in these systems because of the use of the graphical interface [12].

Many authentication systems have been evolved over the years. Today, biometric authentication system holds a prominent place as many users utilize them over textual or graphical based authentication systems. [13] However, one study showed that for mobile authentication, 70% of the users preferred PIN or android graphical pattern even though they are more prone to attacks. The users tend to opt the textual-based method as they don't care about the security but the ease with which they can simply get over with the login phase. Thus, knowing this fact, the attacker will try to break into those systems which use textual or graphical based systems. Besides, biometrics wouldn't be the one used for authentication if the users give more priority to the ease of use when compared to other technologies. Biometrics also lacks privacy, reliability, and security. Thus, the existence of PIN and pattern approaches is present even in the overexposure of biometrics [14].

III. HONEYPOT CONCEPT

In computer terminology, Honey pot is a computer security mechanism set for detecting and counteracting attempts from unauthorized users. Honeypot is designed by the system just to get attracted by the attackers and intruders. The main function of the honeypot is to portray itself as the possible intent for the attackers mainly server to collect information and to report the defenders about the attempts to access the honeypot by intruders. Honeypots are mostly used by cybersecurity research companies and enterprises, to examine and defend their system from being attacked from potential threats. Honeypot is an important implementation tool for business associations and cybersecurity researchers to defend their systems from advanced threat actors.

The working operation of a honeypot mainly deals with computer applications that replicate the functioning of a system, diverse services, and pretend to viewed as the network part. When an intruder tries to log in to the system, the admin will be notified about the threat immediately and the log is generated for all the entries. The intruder becomes successful in logging to the system and stealing information but here honeypot is able to fool the intruder by providing the fake data. The intruder remains unaware about this fool act by then the attacker will be charged for legal actions by the official. So, by this, it is possible to protect our system. Researchers doubt that few cybercriminals tend to apply the concept of honeypot to collect information intelligence about researchers, fake their identity as a lure and mislead by spreading wrong information.

With respect to the design and classification, honeypots are divided into two types: Production and Research. Production honeypots are usually deployed within an organizational environment to protect the organization. They protect the system by giving regular alerts to administrators. Research honeypots are used to gather intelligence on the threats and inspect the hacker activity well in advance and learn how to prevent the systems from attackers and progress. Honeypots can also be classified as low-interaction, medium interaction or high-interaction honeypots. A low-interaction honeypot replicates only the services which are often requested by the attackers and hence they are less risky and easily maintainable. A medium-interaction honeypot involves solving more complex attacks by providing a better illusion of operation systems. A high-interaction honeypot gives practical experience to the attackers by imitating the activities of production systems and representing an ample amount of information.

IV. LITERATURE SURVEY

In [15], a dynamic pin is used as a password so that it becomes difficult for the attacker to break even if he observes while the user types in the password. This system requires less memory and dynamically changes the PIN of the device. Four digits of date and time are used as a password. Different formats such as h1:h2:m1:m2, m1:m2:h1:h2, h2:m1: h1:m2 can be used based on the user's preference. The system cannot be taken down by the brute force as the PIN changes from time to time. Although this system is a good solution for shoulder surfing attack because of the dynamic PIN generation, the shoulder surfer can easily deduce the password if this method gets universally accepted.

Pass matrix [16] protects the user suffering from shoulder surfing in public places through a one-time login indicator. The login indicator which is generated randomly during each phase for pass images will be unused after the session ends. Better security is provided by the login indicator in opposition to shoulder surfing attack because a dynamic pointer is used by the user to identify the location of their password rather than selecting the password directly. In the pass matrix, a part of every image is used as a password from a sequence of n images. In this, the first square is located in the first image and second square in the second image and so on. The user chooses one grid from each image instead of choosing 'n' grid in the same image. The Cued Click Point (CCP) helps the user to remember and recall their password. If the user clicks on an improper password area within the picture the login will be failed. However, the disadvantage is the hacker can deduce the password through concealed cameras.

The randomized keyboard [12] expects the user to type in something which is incorporated with an augmented reality wearable device. The user can see the keys on the randomized keyboard through augmented reality device which is commercially feasible. Different keyboard layout is made visible to the shoulder surfer wherein he cannot deduce the actual keyboard pattern. It is important to make sure that the keystrokes done by the user cannot be easily identified by the shoulder surfer. Even if he does so, the different keyboard pattern misleads the shoulder surfer from knowing the actual password. An algorithm called Individual Key Randomization (IKR) is used to randomize the keys on the keyboard. An algorithm called Row Shifting (RS) is used to shuffle the keys row wise whereas Column Shifting (CS) is used to shuffle the keys column wise. This method overcomes the disadvantages of having a shoulder surfer peak in while the user types in the password. The above three algorithms help the user to efficiently type in the password by misleading the shoulder surfer. However, the user should always wear the augmented reality devices or glasses. [12]

This [17] technique consists of two phases namely registration and authentication phase. During the registration phase, the user is expected to enter his valid username and select images from the given set as his password. Every image is associated with three-digit code where this code has to be entered by the user to choose his image along with direction and the same has to be remembered by the user for the entire process. During the authentication phase, the user is expected to identify the password images and the random code associated with the images. However, for every authentication session the images will be randomized. This technique uses indirect selection such as choosing the image next to password image called the subordinate image. This subordinate image is decided based on the direction chosen initially during the registration process. The correct identification of the subordinate image for every password image from the given set leads to successful authentication else it directs the user to start the whole process again from the beginning. [17]

The proposed ColorPass [18] technique follows the concept of partially observed attacker model where the user can view only the response provided by the system but not the challenge values. Here, the user chooses four pin colors. In the login procedure firstly, the user has to enter his login id and then when the system authenticates the login id it will generate the feature table on the system that throws some challenge values in the range 1 to 10 to the user. The feature table can be selected depending upon the challenge values and further the color pin has to be selected depending upon the feature table that exactly indicates the colour cell. The digit in the color cell has to be identified and submitted as a response to the given challenge by the user. The login process will be completed only after responding similarly to all the other remaining three given challenges. The response given by the user will be

evaluated by the system which then the system finally decides if the user is a legitimate user or not. However, this system does not work for fully observable attacker model [18].

In [21], a concept based on merging images called hybrid images is used wherein this technology simply fools the eyes of the shoulder surfer. The core idea is on the simple observation of the variation in the distance between the screen and the user with that of the screen and the shoulder surfer. The user views the screen from the lesser distance when compared to the shoulder surfer who is at least 0.9 meters away from the screen. Taking this into account, a hybrid keypad is implemented. The keypad consists of numbers with each button being the combination of two digits. The shoulder surfer is misled since the button is totally viewed differently by him with varied layouts. Consequently, the extraction of user's PIN becomes difficult. The shuffling of digits is performed in every authentication. This helps in knowing the spatial arrangement of the digits pressed. The hybrid keypad consists of two keypads. One keypad is viewed only by the user called user's keypad and the other which is visible to the shoulder surfer called shoulder surfer's keypad to confuse him. This hybrid keypad is created by using low pass and high pass filter parameters. This filtering helps in creating two images. The spatial frequency of both the keypads varies which differentiates the keypad layouts. The algorithm used called visibility algorithm helps to find the minimum safety distance from the user's keypad to the shoulder surfer. Therefore, a false PIN layout is created in order to protect the shoulder surfing attack. The disadvantages are - it's too complicated when compared to fingerprint scanner authentication scheme and the third-party apps already use a shuffling scheme which is nearly as complex as Illusion PIN concept [21].

This paper [22] presents a more secured pattern-key based password authentication system where these grid points forms the pattern and these grid points only point to the location of number in an integer matrix. The pattern key being the first level is followed by the secret key and then the dummy values at the last. During the Registration phase, user will be given a 5*5 block grid numbered from 1 to 25. Firstly, the user types in the location number of the pattern. Then in addition to the pattern, the user registers a key for numbers 0 to 9. A key value ranging from "0 to 9" maps to any integers or characters or to any special characters. Followed by this, the user needs to type in the number of dummy values in this phase where dummy values precede as well as succeed the real password values. These dummy values are named as left and right dummy values. During Login phase, after entering the username a next screen appears containing 5*5 grid block will appear with randomly generated numbers. The pattern choose in the registration phase has to be remembered by the user to map the key values to the selected password values along with left and right dummy values and then enter the password. If the password matches it authenticates the user and is able to log in successfully else fails in the login process. The disadvantages are- three secured features are time consuming and remembering a lot of key values during authentication may frustrate the user [22].

In [23], pictures are used as password as the human brain has a capacity to remember hundred images with detail. At the beginning, users are exposed to 50 images out of 70 images wherein each character are assigned to an image. The shoulder surfer cannot easily identify which character is assigned to which image. These images will be from the random art gallery. Here, the user chooses images that are difficult to relate and are colourful. So, for every 10 characters the user selects a picture that signifies a character. The user’s pass images are these 10 images. Also, the user should enter the username. The login phase takes 5 columns and 14 rows of the 70 images. The images displayed during login phase help him to recognize the password character. The account will be blocked after 3 trials. Therefore, [23] provides a secure medium for an authentication system. The disadvantages are – the system is very complicated since it consists of complex images and difficult to remember many images.

V. PROBLEM STATEMENT

Nowadays, there is an increasing usage in web services so the personal business email can be sent to the user when the user gets accessed to the user’s personal information, load files and photos to albums in the cloud or cancel the transaction. Users might not be able to secure the password from the unknown while logging into these facilities. People hack on the whole authentication either by direct supervision or with the help of external devices such as video cameras or a surveillance camera or from the reflected image on the window. Once the intruder acquires the password, it is possible for them to get the personal accounts and that would eventually end in stealing one’s information. The following are the problems:

A. The issue of securing password in public in order to reduce shoulder surfing.
B. The issue of creating secure password efficiently as compared to textual password.
C. The issue of searching the exact image during the login phase becomes tedious.
D. The issue of memorizing the password images at the time of authentication.
E. The issue of having finite usage in authentication applicable only to some devices.

In this paper, we not only explore about the shoulder surfing and the preferences of the user and the hacker may guess the correct password but also, the following assumptions.

1) The client and the server communication are secured by SSL so that the information would not be leaked to the attacker while transmitting.
2) The authentication system between the client and server devices is reliable.
3) The screen and the keyboard of the system are difficult to protect, but an OTC which is sent to the e-mail and the coordinates selected during the registration phase can be protected.
4) Users should register their account in a secure place where there are no observers or the cameras present.

VI. OVERVIEW OF HONEYPASS

HoneyPass is composed of the following components (see Fig 1):

A. Grid Formation Module
B. One-Time-Code Generation Module
C. Horizontal and Vertical Slider Control Module
D. Transmission Module
E. Password Verification Module
F. Honey Pot Module

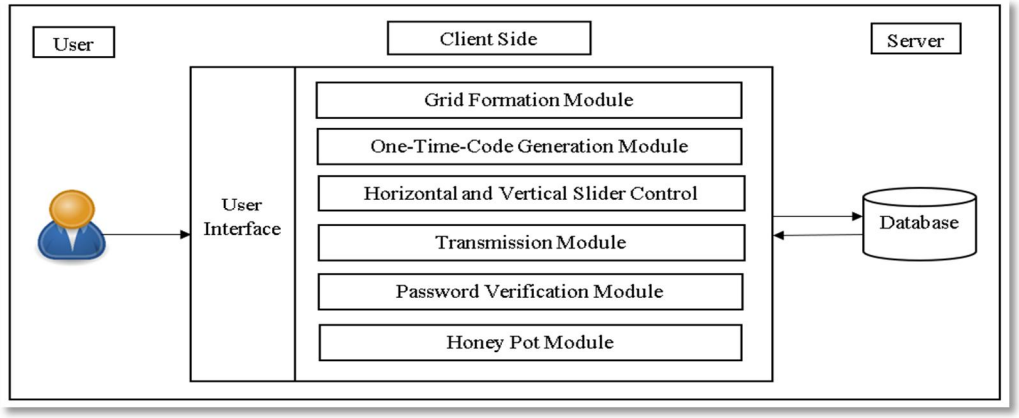


Fig 1: Overview of the HoneyPass System

1) *Grid Formation Module:* This module formulates grids by dividing each image into tiny squares. From the set of formed squares, the user gets to choose one square as a password known as pass-square. The system provides three images divided evenly into a 6x8 grid as shown in the figure. The user needs to select one pass-square from each grid. The larger the image divided, the higher the risk for a brute force attack. However, the formed squares cannot be extremely smaller that makes it difficult for the user to recognize the password image. This difficulty, in turn, might increase the complexity of the user interface. As a result, a 6x8 grid system is selected to make it more user-friendly without having to decrease the concentration of the grid.

Fig 2: Three 6x8 image grids

2) *One-Time-Code Generation Module:* This module generates One-Time-Code (OTC). The OTC consists of three alphanumeric pair. Each pair is a combination of one alphabet from A to F and one digit from 1 to 8. (For example, the three pairs can be C5, B3, E1). The system generates all three pairs randomly. The user gets the OTC through the mail. Each time the user logs in to the system, a new OTC sent to the user. The motto is to keep the password secret from the shoulder surfers by generating a new OTC each time. The pass-squares can be known if the shoulder surfer gets to know the OTC. However, gaining access to OTC is a lot harder than imagined.

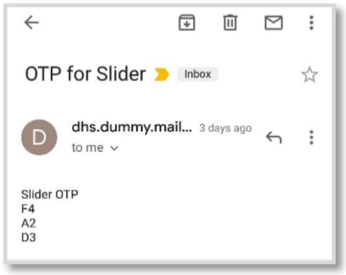


Fig 3: Obtained OTC

3) *Horizontal and Vertical Slider Control Module:* The system consists of two sliders: horizontal slider and vertical slider. As shown in the figure, the horizontal slider includes alphabets from A to F, and the vertical slider includes numbers from 1 to 8. The user can shift one character at a time with the help of arrows. The arrows help the character move in all directions, i.e., up, down, right, left. From the obtained OTC, the horizontal slider is shifted to the respective pass-square's column, and the vertical slider is shifted to the pass-square's row. Therefore, the slider implicitly leads to the user's pass-square location.

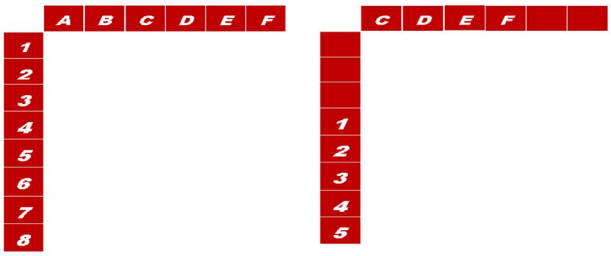


Fig 4: Before Sliding and After Sliding

4) *Password Verification Module:* This module verifies the password entered by the user in the form of slider movement. To get authenticated, it is important to align the slider's character with the pass-square. This alignment is performed with the help of obtained OTC. Once the user locates the slider character to the respective column and row, the user will be able to login to the system. The details of how the slider is aligned to the pass-square will be discussed in the next section.
5) *Transmission Module:* This module transmits information from the client to the authentication server. In this case, the pass-squares are transmitted to check for authenticity. The authentication server stores the user's pass-squares in the database. These pass-squares are matched with the ones the user submits. Once the pass-squares match, the user will be able to login to the system. SSL (Secure Socket Layer) protocol protects the exchanged information from being intercepted and stolen.
6) *Honey Pot Module:* Once the user logs in to the system, he can upload and download files from the cloud. To download any file, the user requires to enter the passkey. This passkey which is known only to him is sent to the user's mail when he uploads the file which is shown in the figure. When the hacker tries to gain access to the user's private file, the system limits the login attempts to three. However, a duplicate file is downloaded when a wrong passkey is entered after three attempts.

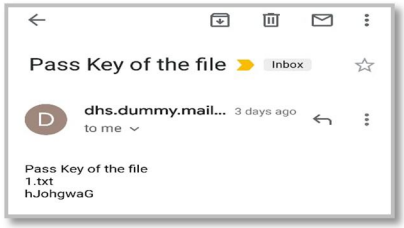


Fig 5: Obtained Passkey

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

VII. HONEYPASS: THE PROPOSED SYSTEM

The HoneyPass's authentication consists of two phases such as registration phase and login phase. The description is as given below:

A. Registration Phase

In this phase, during the creation of an account, the user requires to enter all the required information such as user id, username, password, valid email-id, etc. Once all this information is submitted, three random images appear in three consecutive pages divided into 6x8 grid wherein the user has to select one coordinate image square from each page as the graphical password to get authenticated in the login phase. The three coordinates selected will be concatenated together to generate a hash code and the same will be stored in the database for reference.

B. Authentication Phase

During login phase, registered user logs in to the system by using his authenticated user id and password, if both matches one-time-code (OTC) will be received by the user immediately to his email id. OTC contains the random pair of horizontal and vertical slider coordinate points for all the three images. Using Coordinates received in OTC the slider has to be adjusted to match with the coordinates chosen by the user during the password setting phase. Once the hash code created while registration matches with the generated hash code, user will be successful in logging in to the system and enter in to the home page else, process ends and login page will be displayed again.

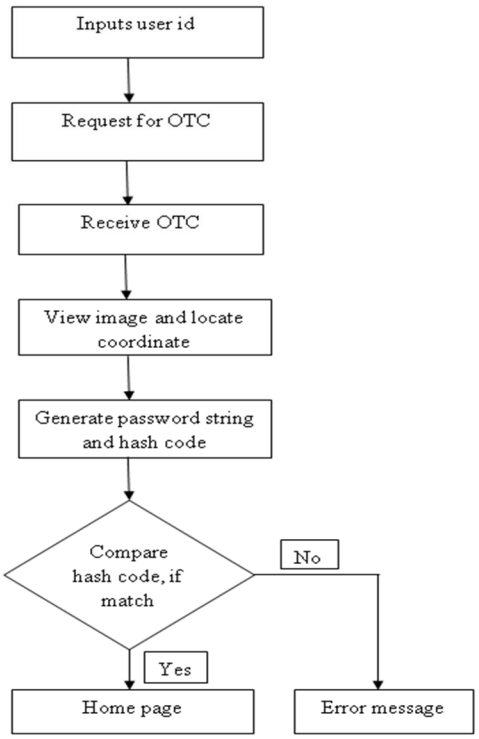


Fig 6: Flowchart of Registration Phase.

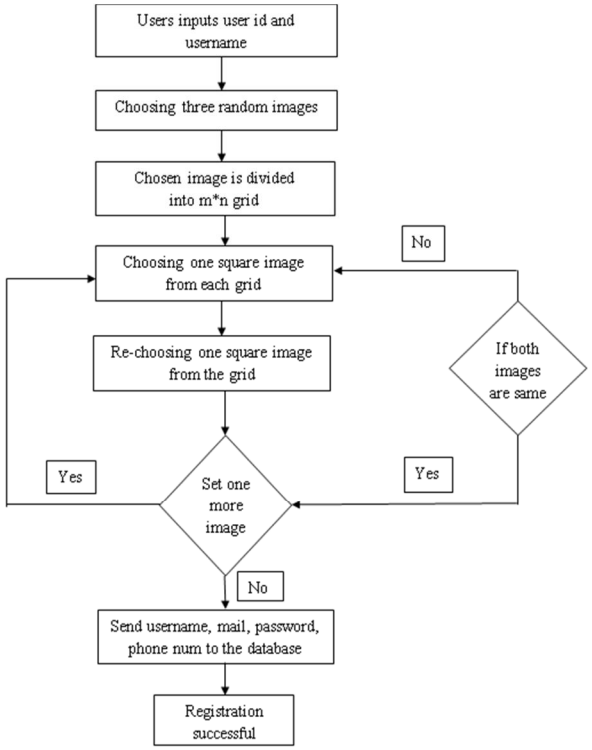


Fig 7: Flowchart of Authentication Phase.

Fig 6 is the flowchart of registration phase and the following describes the **registration** steps in detail-

1) The user inputs his credentials such as user id and user name and requests for registration.
2) Server randomly chooses three images and breaks it into an m*n grid format.
3) The user selects one square image from each grid and those coordinates have to be remembered by the user.
4) Once the pass-square has been chosen from each grid by the user, the password string is created and the hashtag is generated.
5) Hence, the registration process becomes successful and all the details about the user such as user id, user name, email id, and phone number are automatically stored in the database for future reference.
6) A confirmation message about the successful registration is displayed to the user.

Fig 7 is the flowchart of authentication phase and the following describes the **authentication** steps in detail-

1) The user needs to enter the same user id that was registered during the registration phase.
2) User requests for OTC to receive a One-Time Code to his mail.
3) Once the OTC is received, the server again chooses three random images and displays it to the user for authentication.
4) The user has to slide the coordinate points with the help of the slider and locate to the correct coordinate points using the OTC.
5) The password hence created generates a hash code.
6) The comparison is made between the currently generated hash code and the existing hash code during password setting.
7) If they both are equal user will be given an entry to the home page else error messages will be displayed.

VIII. IMPLEMENTATION

The HoneyPass prototype was built using the IDE Eclipse Galileo. The client side is designed using Java and Servlet, JSP to implement the functions that check for registered users and matching password, the creation of password images, grid formation, one-time-code delivery, and the horizontal and vertical slider control system. The server side is implemented using Tomcat 7.0 and My-SQL 5.0. The driver used for JDBC connection is Type 4 - Driver. The registered users and pass-squares stored in the database are fetched during the authentication phase. The stored details help in password verification.

In our implementation, the database is uploaded with a set of predefined password images. However, the system supports users' upload action. Each image is divided into a 6x8 grid system wherein the user selects three images as a password during the registration phase. From each of the three images, one square is chosen as a password. The actions performed during the registration phase is shown in the Fig 8 and Fig 9.

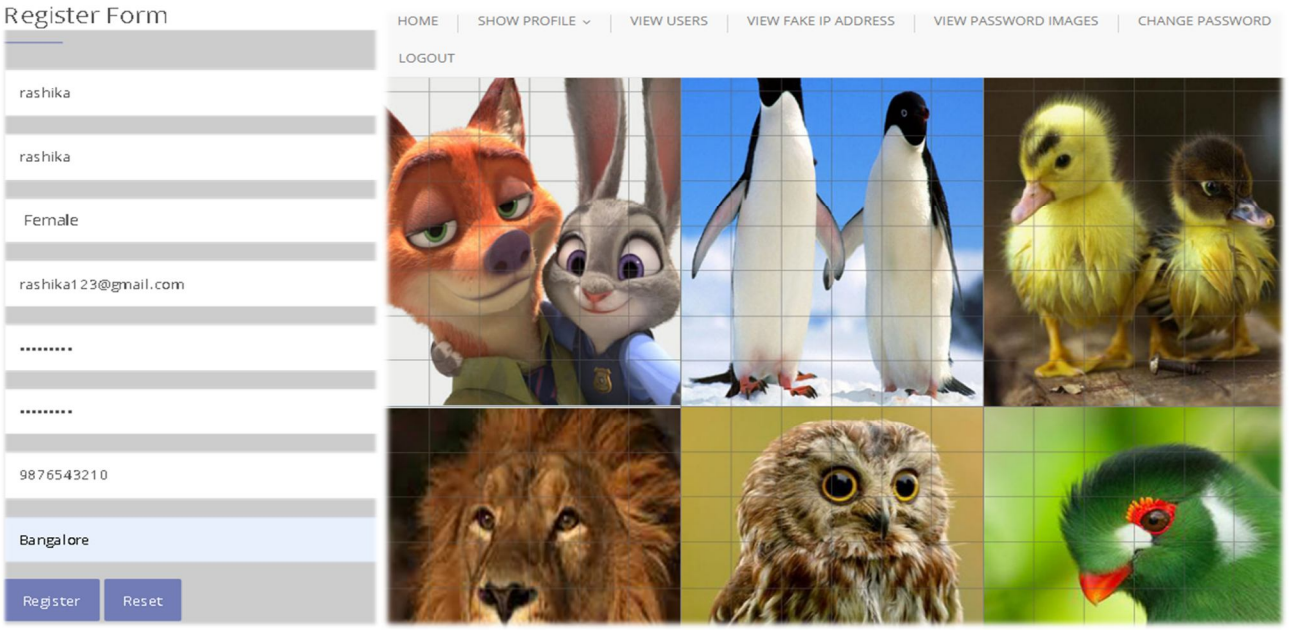
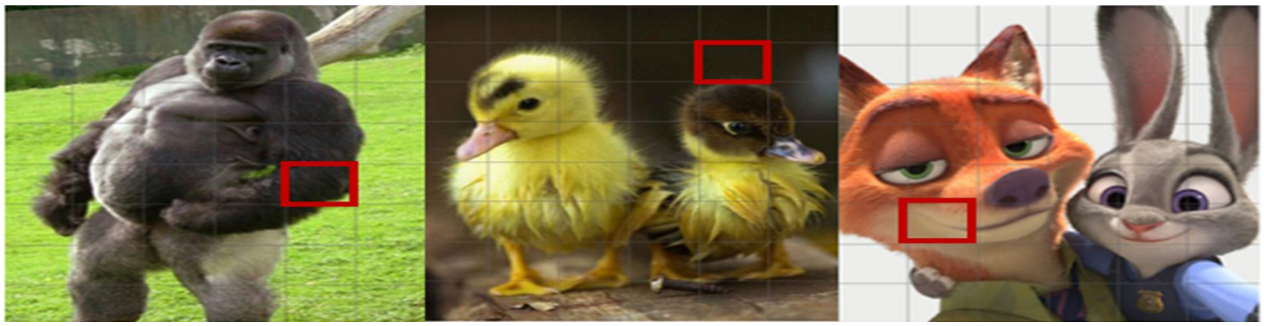


Fig 8: (a) User's registration form. (b) Set of predefined password images stored in the database



(a) Image 1 (col=5, row=5) (b) Image 2 (col=5, row=2) (c) Image 3 (col=2, row=6)

Fig 9: Selected Pass-squares.

The first step in the login phase is to get the one-time-code as shown in the Fig 10. This code is sent to the user's email as soon as he requests for it. To protect against shoulder surfers, the user can check the obtained OTC from his smartphone. The next step is to match the coordinates of the pass-squares to the obtained OTC. The user has to match coordinates of the first image with the first alphanumeric pair in OTC, coordinates of the second image with the second alphanumeric pair in OTC and coordinates of the third image with the third alphanumeric pair in OTC. The match actions are performed using the horizontal and the vertical slider as shown in Fig 11.

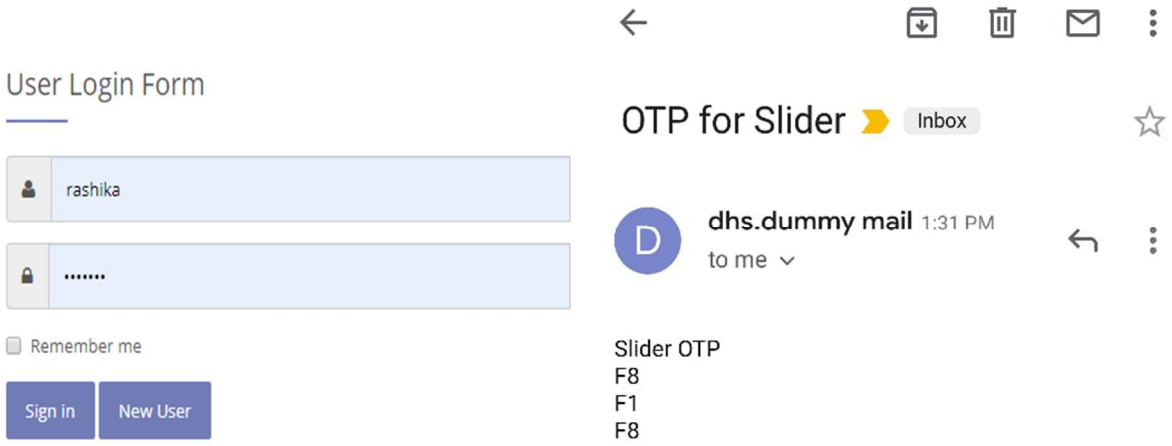


Fig 10: (a) Login Form (b) Received OTC that has to be matched with the pass-squares coordinates

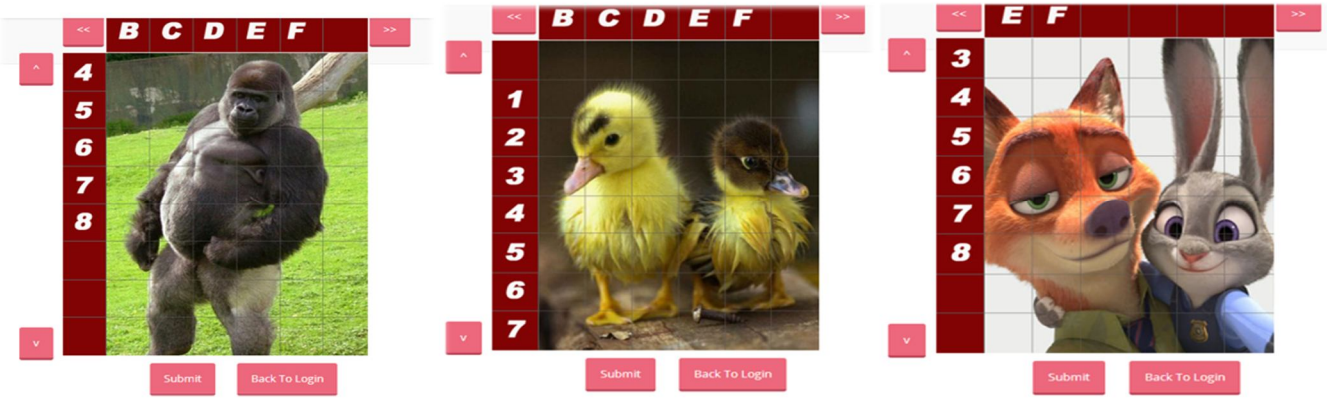


Fig 11: Match action using the horizontal and the vertical slider

Once the user logs in to the system, he can upload and download files to/from the system. To download the uploaded file, the user requires the passkey sent to his mail as shown in the Fig 12. The user has to enter the received passkey to download the file (Fig13). Even though the shoulder surfer steals the OTC, he will not be able to download the file. The honeypot concept prevents the shoulder surfer from accessing the file. When he tries to gain access to the user's private file, the system limits the login attempts to three. However, a duplicate file is downloaded when a wrong passkey is entered after three attempts.

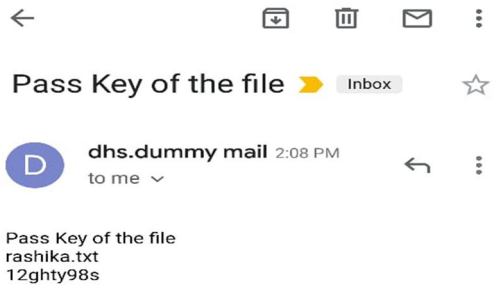


Fig12: Obtained Passkey

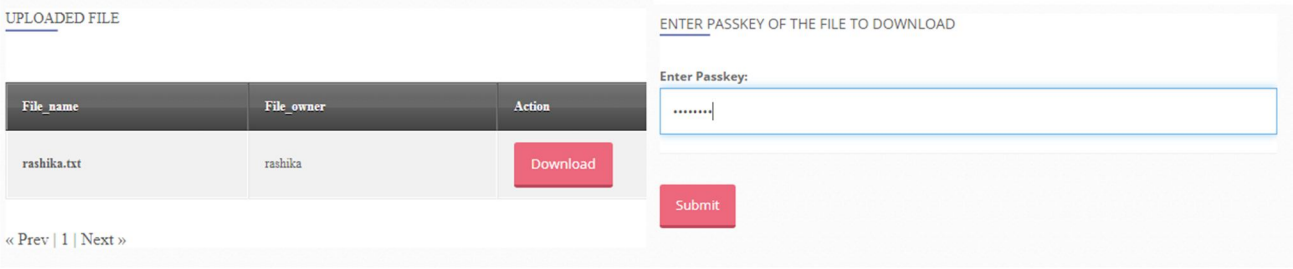


Fig 13: (a) Uploaded file by the user (b) Passkey is entered to download the file

IX. CONCLUSION

In this paper, the cause for shoulder surfing attack and the prevention methods is put forth. An attempt that has been made to contemplate the significance of various graphical authentication systems that have been proposed over the years to overcome shoulder surfing attacks. The methods to overcome the disadvantages of textual passwords are presented. The system's advantages and disadvantages that have been surveyed are presented for each paper. The need for graphical authentication system is emphasized. Implementation of the honeypot is addressed here to secure the system from counteracting attempts of unauthorized users to steal the information. Like any other graphical authentication system, HoneyPass is also vulnerable to random guessing attacks but it is strongly resistant to any form of shoulder surfing attacks i.e. either direct observation or with the help of external devices. This approach will help various research analysts to move forward with the graphical authentication system who was unfortunate about the textual password system and their drawbacks.

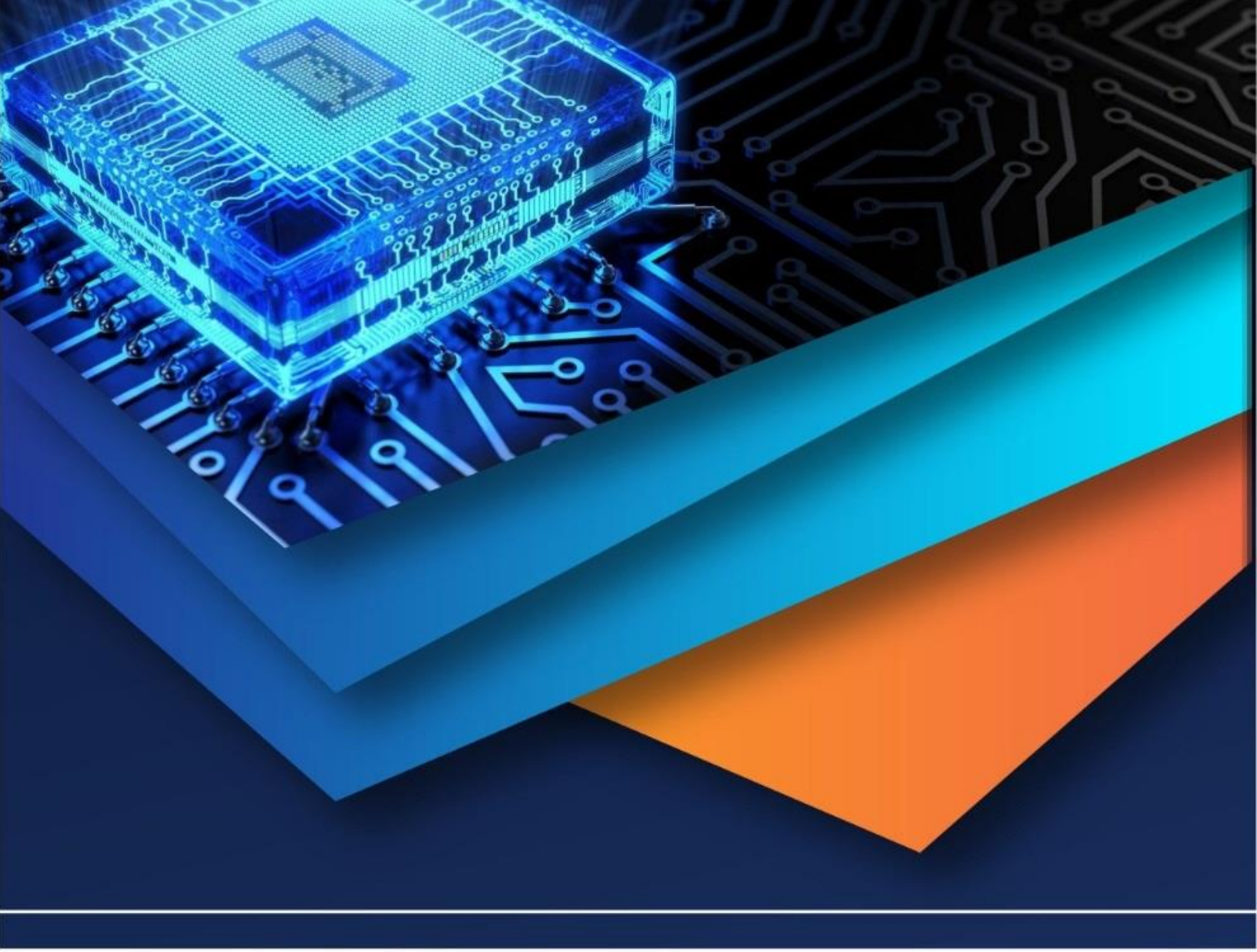
REFERENCES

[1] Mayuri Gawandi, Saloni Pate, Pokhara Snehal, Prof.Said S.K: A Survey on Resisting Shoulder Surfing Attack Using Graphical Password. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 10, ISSN: 2278 – 1323, October 2017.
[2] Aishwarya N. Sonar, Purva D. Suryavanshi, Pratiksha R. Navarkle, Prof. Vijay N. Kukre: Survey on Graphical Password Authentication Techniques. International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 02 | Feb-2018.
[3] MalinEiband, MohamedKhamis, EmanuelvonZezschwitz, HeinrichHussmann, FlorianAlt: Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. The CHI Conference on Human Factors in Computing Systems (CHI 2017), At Denver, CO, USA,2017.
[4] K. Divyapriya, Dr.P. Prabhu: Image Based Authentication Using Illusion Pin for Shoulder Surfing Attack. International Journal of Pure and Applied Mathematics Volume 119 No. 7 2018, 835-840,2017.
[5] Choi, D., Choi, C., & Su, X: Invisible Secure Keypad Solution Resilient against Shoulder Surfing Attacks. International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). doi:10.1109/imis.2016.77, 2017.
[6] Miss. Priyanka Nimbalkar, Miss. YashashriPachpute, Mr. Nishiket Bansode, Prof. Vaishali Bhorde: A survey on shoulder surfing resistant graphical authentication system. Open Access International Journal of Science and Engineering, Volume 2, ISSN (Online) 2456-3293, December 2017.
[7] Vijayakumari Rodda, Gangadhar Rao Kancherla, Basaveswara Rao Bobba: Shoulder-Surfing Resistant Graphical Password System for Cloud. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, pp. 6091-6096, Number 16 2017.
[8] J. Thirupathi: A Comprehensive Survey on Graphical Passwords and shoulder surfing resistant technique analysis. IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
[9] Dhanashree Chaudhari: A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 11, November 2015.
[10] Monali Pawar, Prof. G.S Mate, Soni Sharma, Sonam Gole, Snehal Patil: A Survey Paper on Authentication for Shoulder Surfing Resistance for Graphical Password using Cued Click Point (CCP). International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 1, January 2017.
[11] M. S. A. Noman Ranak, Saiful Azad, Nur Nadiah Hanim Binti Mohd Nor, Kamal Z. Zamil: Press touch code: A finger press-based screen size independent authentication scheme for smart devices. PLoS ONE,12(10): e0186940, October 30, 2017.
[12] Peng Foong Ho, Yvonne Hwei-Syn Kam, Mee ChinWee, Yu Nam Chong and Lip Yee Por: Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information. Scientific World Journal, Volume 2014.
[13] Su, X, Wang, B, Zhang, X, Wang, Y, & Choi, D: User biometric information□based secure method for smart devices. Concurrency and Computation: Practice and Experience, 30(3), e4150. doi:10.1002/cpe.4150, 2017.
[14] John T. Davin, Adam J. Aviv, Flynn Wolf, Ravi Kuber: Baseline Measurements of Shoulder Surfing Analysis and Comparability for Smartphone Unlock Authentication. CHI 2017, Denver, CO, USA, May 6–11, 2017.
[15] Yogadinesh S, R. Sathishkumar, Akash L, Aakash V, Kishore Kumar K, Harichander S: Counterfeit shoulder surfing attack using random pin. International Journal of Pure and Applied Mathematics, Volume 118 No. 22, 2018.
[16] M. Kannadasan, J. Amarnadha reddy, K. Venkat Raman: Shoulder Surfing Resistant Graphical Authentication System. International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017.
[17] Swale Saeed and M Sarosh Umar: PassNeighbor: A Shoulder Surfing Resistant Scheme. International Conference on Next generation Computing Technologies Dehradun, October 2016.

[18] Gopika Anil, Chippy, Mary John, Pradeep P Mathew: Color Combo: An authentication mathod against shoulder surfing attack. International Journal of Computer Science and Information Technology Research, Vol.4, Issue 2, pp:(142-147), Month: April-June 2016.
[19] Andrew Lim Chee Yeung, Bryan Lee Weng, Wai, Cheng Hao Fung, Fiza Mughal, Vahab Iranmanesh: Graphical password:Shoulder-surfing Resistant using Falsification. 9 th Malaysian Software Engineering International Conference, Dec 2015.
[20] Shruthi V: CRASH-Cued Recall Based Authentication Resistant to Shoulder Surfing Attack. Online Internatinal Conference on Green Engineering and Technologies Kerala, 2015.
[21] Athanasios Papadopoulos, Toan Nguyen, Emre Durmus: llusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images. IEEE Transactions on Information Forensics and Security,2017.
[22] M Hamza Zaki, Adil Husain,m Sarosh Umar, Muneer H Khan: Secure Pattern-Key Based Password authentication Scheme. International Conference on Multimedia,Signal Processing and Communication Technologies,2017.
[23] Elham Darbanian and Gh. Dastghaiby fard: A Graphical Password against Spyware and Shoulder Surfing Attacks. Malaysian Software Engineering International Conference, Dec,2015

About The Authors

	Arun Kumar S Assistant Professor Dept. of Computer Science & Engineering Sapthagiri College of Engineering Bengaluru - 560057
	Renu R Student (B. E.) Dept. of Computer Science & Engineering Sapthagiri College of Engineering Bengaluru - 560057
	Rashika R Student (B. E.) Dept. of Computer Science & Engineering Sapthagiri College of Engineering Bengaluru - 560057
	Ramya R Student (B. E.) Dept. of Computer Science & Engineering Sapthagiri College of Engineering Bengaluru - 560057



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY