User Persuasion towards Passwords

Graphical Text Passwords

Mr. Raj Mohammed Mohd [1], Dr.C.Shoba Bindu[2],Dr. D.Vasumathi [3]

[1]Asst.Professor, Department of C.S.E, GITAM University,Hyderabad, Telangana, India.

[2]Assoc.Professor,Head, Dept of C.S.E,JNTUA CE,Anantapuramu,AP, India

[3] Professor, Dept of C.S.E,JNTUH CE,Hyderabad,Telangana, India

Email :raaz.mohd@gmail.com [1], shobabindhu@gmail.com [2],vasukumar_devara@yahoo.com[3]

Abstract

Now days, most of transactions can be done through on line in our daily life because of evolution of Internet. There is a necessity to offer the security by means of user authentication, which is a prime factor of any secure system. This paper focuses on usability along with the security features using graphical password authentication, where the images are used as passwords. We propose a secure user authentication using graphical text, which is resistant to capturing attacks and social engineering attacks as discussed in [4]. This paper gives an impact to user with user's persuasion to choose language script, which is visible on a grid as password. This paper introduce a novel approach to improve user's persuasion by using text in the form of graphics and it is displayed like a graphical password and stored in the form of graphics. User authentication with graphical text is resistant to brute-force, guessing, capturing, dictionary and social engineering attacks. In this paper, we compare the usability and security issues of various user authentication methods as per the Josephet. al usability and security features as discussed in paper[8].

Keywords-Passwords; Graphical Text Passwords; Graphical Passwords; Usability and Security.

I. INTRODUCTION

In user authentication, user can prove his or her identity with password to get the system or resources. In general, Most of user authentication methods uses PINs or Text Passwords access to the system or resource. But, these traditional password approaches leads to various vulnerabilities such as guessing, shoulder-surfing, sharing through media (social engineering), brute-force search through automated tools, dictionary attacks with available dictionaries and spyware with key loggers and mouse listener programs.

Alternative to Textual Passwords, Graphical passwords first proposed by G.E Blonder in 1990[1] to meet the long-term memory for remembering the passwords by the users. This is a first foremost step towards User's Persuasion to remember them easily for long-term

Birget formulated the password problem which is having two conflicting requirements i.e. passwords should easy to remember, and the authentication protocol should executable quickly and easily by humans and passwords should secure, i.e., they should look random and hard to guess.

In order to solve this problem, Researchers had gone for graphical authentication schemes, which are alternative to textual passwords to improve the usability and security issues. In a typical graphical authentication scheme, user selects pictures as his or her password when of enrollment. When logging to the system, user need to click on the correct sequence of pictures by recognizing the previously chosen images as password. Human beings are good at recognizing the faces, icons and pictures than words. These are easy to remember and may difficult to crack by means of automated tools. However, Graphical passwords are vulnerable to shoulder-sur~~fing attacks [3~~][9].

We propose a novel cognition based graphical password scheme and designed with challenge response protocol and depends on the user's knowledge to select the passicon from hand hidden keypad. This scheme may also resistant to shoulder-surfing, brute-force attacks and less chance for guessing attack. This scheme also applied to the ATMs, PDA s and Mobile devices.

The rest of the paper organized as follows: In Section 2, we review related work for existing authentication schemes, Section 3 discuss the graphical text password scheme, and Section 4 analyzes the usability and security issues of the proposed scheme, finally concludes in Section 5.

II. RELATED WORK

User authentication is process of determining the whether the user is valid or not. In this process, User should enter his or her User ID and Password which is proof of an Identity of the user. Most of User authentication schemes proposes with Traditional Text Passwords because of their easy use and easydeploy ability over all kinds of environments such as websites, PCs, PDAs, ATMs and Secure Systems etc.

Birget formulated Password problem,which consists of two conflicting requirements. One password must easy to use and remember for long-term and the two password should hard to guess and crack it by means of automated tool like jtr(John The Ripper) etc.

ISBN : 978-93-85100-08-6

To solve password problem, Graphical password concept is introduced by Researchers making use of Image Icons, objects, faces as passwords. These passwords are easy to remember and hard to guess and crack with automated tools.

User authentication methods are classified based on the type of password, which is used for authentication purpose. Password can be generated by means of the following three categories such as Text Passwords, Graphical Passwords and Hybrid Passwords.

The first group of passwords, Text Passwords is mostly used by the users for various commercial, academic and banking applications for the advantage of flexibility of simplicity, easy to use passwords. These text passwords are simple, short in length and can remembered for short time of span. These are well-known for various vulnerabilities such as brute-force search, dictionary, guessing, social engineering attack and capturing attacks (shoulder-surfing, spyware). In order to authenticate to a secure internet banking service, User should under gone with various challenges like transaction password ,OTP generation , CAPTCHAs , challenges related to personal information which impact on login time of user and process may involve number of tokens or factors such as mobile, smart card with details etc.

User authentication methods are designed with good security benefits and not bother about usability for the users and system as well. The researchers have gone for second type of passwords, which solve a password problem and provide usability benefits for the users. In User authentication using graphical passwords, the user need to generate or create a password by selecting images or pictures from Image portfolio in sequence(recognition based mechanism) , sequence of click regions over picture (cued recall based mechanism) , draw a secret on a grid(recall based mechanism) to authenticate the system. These passwords are resistant to brute force search, dictionary attacks, social engineering attacks and these are vulnerable to guessing attacks, spyware, shoulder-surfing attacks.

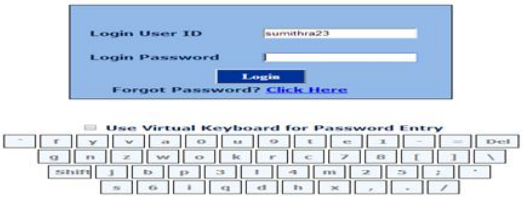
The third class of passwords further classified as Text passwords with Tokens, Text passwords with graphical-assistance, Texto'graphic Passwords and graphical text passwords.

A. Text Passwords with Tokens

In this category, we combine both text passwords with a token (smart card) to offer a better security. Most of the two-factor authentication methods are proposed by researchers in this context. But, these are suffers from usability problems such as remembering the password for long-term and security problems like identity theft. The tokens may be a mobile, smart card or biometric object. These methods enhance both usability and security for the system. But , they are lacking in ID theft and Deployability problems.

B.Text Passwords with Graphical Assistance

Some of the User authentication methods designed with text passwords with graphical-assistance with dynamic and static virtual keyboard mechanism, persuasive text passwords, where user can get the hint for the password when login to system.



Login User ID: sumithra23

Login Password
Login
Forgot Password? Click Here
□ Use Virtual Keyboard for Password Entry
` f y v a o u 9 t e 1 - = Del
g n z w o k r c 7 8 [ ] \
Shift j b p 3 l 4 m 2 5 ; '
s 6 i q d h x , . /

Fig 1: User Authentication with Virtual QWERTY Keyboard with Random Placement of Characters

As shown in the Figure 1, User has a provision to use Virtual Keyboard for password entry to avoid the spyware attacks with Key loggers, which records the keystrokes from keyboard to get password. But, Static virtual keyboard is vulnerable to shoulder-surfing by direct observation of User login process. In the above figure, they have used to dynamic virtual keyboard, where place of letters have been randomly on QWERTY keyboard. But, Dynamic virtual keyboard still suffers from shoulder-surfing because user need to click on letters displayed on the screen. When user clicks on the letter, there is a chance to get the password by attacker's direct observation. To confuse the surfer, virtual keyboard can replace positions of characters randomly on the screen. But, it is still vulnerable to shoulder-surfing attack by means of cameras to record the login process. From a record of login process, attacker can get the password.

User authentication with Dynamic virtual keyboard also suffers from the capturing of login through internal software or spyware such as key loggers and mouse listeners.These passwords mostly suffer from little vulnerability of text passwords.

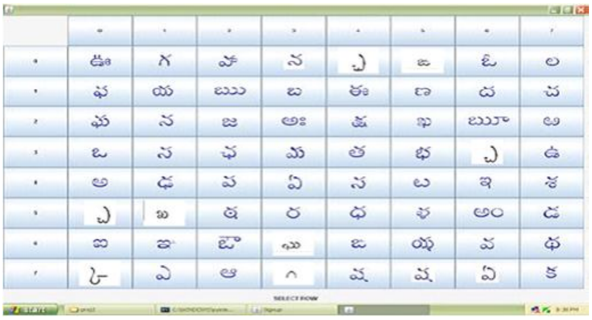
C. Text' O graphic Passwords

In this, we can combine text and graphical elements in a password as discussed by Misbahuddin[11]. Some of user authentication methods are accepts both graphical password and text passwords. User need to remember both text password and graphical password which leads to a usability problem. There is a chance to have vulnerabilities of both text and graphical passwords.

In this paper, we propose a novel approach with graphical text, which is a text in the form of graphics. Text is visible on a grid like a graphical element and gives a cue to the user for remember and recognize easily and it is stored in the form of graphical element which require more storage space to counter brute-force and dictionary attacks. In this paper, we illustrate Graphical Text password mechanism as specified in [4]. User authentication method with pass script revised and analyzed for efficient analysis of usability and security of user authentication methods.

III. USER PERSUASION TOWARDS PASSWORDS

This section deals with an improved cognition based authentication scheme [4], which is resistant to both shoulder-surfing attacks and spyware attacks. This scheme designed with C-R protocol where the set of challenges are given to the user to prove his identity with a password which is a combination of graphical elements of telugu script. This mechanism helps us to make an interest towards their own mother tongue language. This method is useful and applicable for any kind of language which is having script and a grammar. In this scheme, the graphical elements used in authentication are letters shown in a window on the screen as shown in fig 2.



	ఊ	గ	పా	న	[illegible]	ఙ	ఓ	ల
	ఫ	య	ఋ	బ	ఈ	ణ	ద	చ
	ఘ	న	జ	అః	ఝ	ఖ	ౠ	ఱ
	ఒ	స	ఫ	మ	త	భ	[illegible]	ఉ
	అ	ఢ	వ	ఏ	స	ట	ఇ	శ
	[illegible]	ఙ	థ	ర	ధ	ళ	అం	డ
	ఐ	ఔ	ఔ	[illegible]	ఙ	య్య	వ	థ
	[illegible]	ఎ	ఆ	[illegible]	ష	ష	ఏ	క

SELECT ROW

Fig 2: User Login Window using Telugu letters on 8x8 Grid.

For example, User wants to choose a password with telugu letter '?', he or she has to remember the letter. Now the user needs to enter the position of that letter '?' ,which is changed time to time to avoid the shoulder surfing and spyware attacks. This scheme designed to motivate the users to log in quickly and accurately in a game like fashion with known letters of their mother tongue language. The login takes place in a series of challenge-response rounds up to length of password. The number of rounds is equal to the number of passscript elements selected by the user, so this is easily changed, with more rounds providing higher security. In order to remember the password, we can use the telugu text phrases like "" .

In this case, user can choose the first letters of every word in red color. Here, user need to remember the letter in graphics format and letter picture stored in the database along with pass string generated for that letter. In a password field, we are not storing the uni code which is necessary to display that in a text file instead we are storing the image pertaining to that letter. For the images, there is no brute force and dictionary attacks because of an availability of dictionaries for textual images. Figure 2 displays password login window, where the letters of telugu language are displayed on a 8X8 grid with 64 letter symbols.

IV. ANALYSIS

In this section, we have analyzed Graphical text password scheme with usability, security and deployability benefits, which are discussed in[8] and compared with existing schemes. As discussed in paper [8], there are three categories of benefits which influence the user's persuasion towards passwords:

- Usability
- Deployability or Accessibility
- Security and Privacy

These benefits for graphical text password analyzed and compared with various schemes by giving the ranking as listed in paper [8].

A. Usability Benefits

This section discusses the usability benefits such as Memory wise Effortless, scalable for users, Nothing to carry, Physically Effortless.

Memory wise-Effortless: Users of the scheme do not have to remember any secrets at all. We grant a Quasi-Memorywise-Effortless if users have to remember one secret for everything (as opposed to one per verifier or a server).

Scalable-for-Users: If we increase the user accounts for a system then it doesn't make a burden for the user to use the system or resources. As the mnemonic suggests, we mean "scalable" only from the user's perspective, looking at the cognitive load, not from a system deployment perspective, looking at allocation of technical resources.

Nothing-to-Carry: Users do not need to carry an other physical object such as an electronic device, mechanical key, and piece of paper to get access to the system. Quasi-Nothing-to-Carry is awarded if the object is one that they'd carry everywhere all the time anyway, such as their mobile phone, but not if it's their computer (including tablets). Most of the token based user authentication methods don't offer this benefit.

Physically-Effortless: User authentication offers this benefit, when user can log in to the system without physical effort beyond, pressing a button and like typing a large password, memorizing the actions, entities or password to prove his or her identity. Schemes that don't offer this benefit include those that need typing, scribbling or performing a set of motions. We grant this benefit, Quasi-Physically-Effortless if the user's effort limited to speaking, on the basis that even illiterate people find that natural to do.

Easy-to-Learn: This benefit offered by the schemes which doesn't require a training to enroll or enter password. Users who don't know the scheme can figure it out and learn it without too much trouble, and then easily recall how to use it. Most of Text based user authentication methods offers this benefit.

Efficient-to-Use: The time the user must spend for each authentication is acceptably short. The time required for setting up a new association with a verifier, although possibly longer than that for authentication, is also reasonable. If the login or registration time of login process is short to spend less time, then used by large number of users efficiently.

Infrequent-Errors: If the scheme is away from false positives or true negative errors then it doesn't offer this benefit. The task that users must do to log in usually succeeds when performed by a legitimate and honest user. In other words, the scheme isn't so hard to use or unreliable that genuine users are routinely rejected. Most of user authentication methods offer this benefit.

Easy-Recovery-from-Loss: if the scheme facilitates the change password, forgot password option without much effort of the user then that scheme offers this benefit. This combines usability aspects such as: low latency before restored ability; low user inconvenience in recovery; and assurance that recovery will be possible, such as via built-in backups or secondary recovery schemes. If recovery requires some form of re-enrollment, this benefit rates its convenience.

The analysis of usability benefits for various user authentication methods captured in the figure 2.

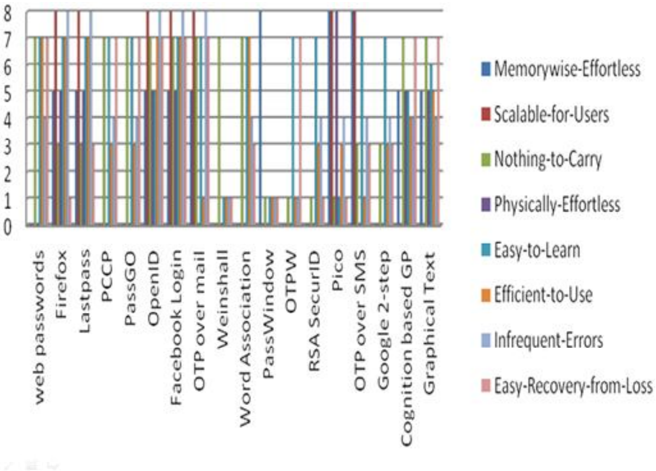


Fig 3: Usability benefits of various user authentication methods.

Graphical text password have almost same ranking as similar to graphical password methods like PCCP[10](cued recall),PassGo(recall),cognition based GP(recognition). Graphical Text ensures the easy learning capability and Efficient to Use with native language script by more number of users.

B. Deployability Benefits

There are some user accessibility benefits offered by various user authentication methods listed below.

Accessible: Users who can use passwords are not prevented from using the scheme by disabilities or other physical conditions not knowledge of the user. Most of token based schemes depends on biometrics and accessible by all kinds of users.

Negligible-Cost-per-User: In the user's perspective, user doesn't spend money to use the system. The total cost per user of the scheme, adding up the costs at both the prover's end (any devices required) and the verifier's end (any share of the equipment and software required), is negligible. The scheme is plausible for startups with no per-user revenue.

Server-Compatible: At the verifier's or server end, the scheme is compatible with text-based passwords. Providers don't have to change their existing authentication setup to support the scheme.

Browser-Compatible: Users don't have to change their client to support the scheme and can expect the scheme to work when using other machines with an up-to-date, standards-compliant web browser and no other software or plug-ins. The schemes fail to offer this benefit, in the event that they need installation of plug-ins or any sort of software whose installation requires administrative rights. The schemes offer Quasi Browser-Compatible if they rely on non-standard but very common plug-ins, e.g., Flash.

Mature: If the scheme that implemented and deployed on large-scale for real authentication purpose beyond the research, then Indicators to consider for allowing the full benefit may also include whether the scheme has experienced user testing, whether the standards community has published related documents, whether open-source projects executing the scheme exists, whether anybody other than the practitioners has adopted the scheme, the amount of literature on the scheme and so forth..

Non-Proprietary: Anyone can make or use the scheme for any purpose without having to pay royalties to anyone else. The relevant techniques are generally known, published openly and not protected by patents or trade secrets.

We have compared and analyzed user authentication methods for deployability benefits by giving the ranking and shown in given figure 4.

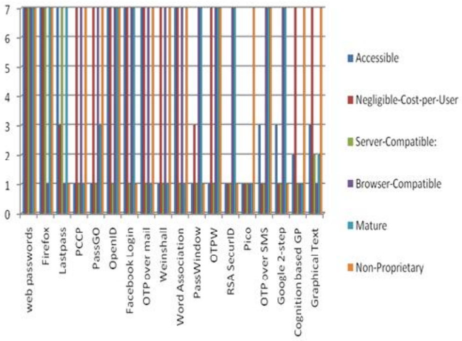


Fig 4: Deployability benefits of various user authentication

methods.

The deployability benefits for graphical text password as similar to graphical password methods and it gives some maturity for user use their own language script as password in the form of graphics.

C. Security Benefits

The security benefits are the services offered by a user authentication method to counter various security vulnerabilities or attacks. There are some benefits listed along with rating procedure for user authentication method.

Resilient-to-Physical-Observation: This benefit ensures to resist an attacker to get a password after observing login process and later authenticate as a valid user. This service counter the shoulder-surfing attack by physical observation or by an external entity camera.

We can rate quasi Resilient-to-Physical-Observation if the scheme could be broken only by repeating the observation more than, say, 10-20 times. Attacks include shoulder surfing, filming the keyboard, recording keystroke sounds, or thermal imaging of keypad.

Most of the user authentication methods with text, recall and cued recall graphical password doesn't offer this benefit where as few of the recognition based graphical passwords offers this benefit. User authentication with Graphical text password offers this benefit by Quasi-resilient to Physical Observation.

Resilient-to-Targeted-Impersonation: This benefit offers the users from guessing attacks done by a skilled investigator, who get the password by exploiting knowledge of personal details (birth date, names of relatives etc.) of specific user. A user authentication method which depends on personal knowledge queries to recover the password doesn't offer this benefit.

Resilient-to-Throttled-Guessing: This benefit counters attacks done by an automated guessing of passwords through an online server, through a chip, a process which makes throttling repeated set of requests. Lack of this benefit is to penalize schemes in which it is frequent for user-chosen secrets selected from a small and low min-entropy. Most of the user authentication methods doesn't offer this benefit fully if it allows a chosen secrets.

Resilient-to-Unthrottled-Guessing: The rate of guessing constrained only by available computing resources cannot successfully guess the secrets of a significant fraction of users.

Lack of this benefit is to penalize schemes,where the space of credentials is not large enough to withstand brute force search for dictionary, rainbow tables and related brute force methods smarter than raw exhaustive search, if credentials are user-chosen secrets. The schemes which are not resistant to dictionary, brute force search attacks don't offer this benefit.

Resilient-to-Internal-Observation: This benefit offered by user authentication which are resistant to Man In The Middle attacks, Spyware and replay attacks. We grant this benefit with Quasi-Resilient-to-Internal-Observation if the scheme could be broken only by intercepting comments or eavesdropping clear text more than, say, 10-20 times. This benefit assumes that general purpose devices like software-updatable personal computers and mobile phones may contain malware, but that hardware devices dedicated exclusively to the scheme that made malware-free.

We rate Quasi-Resilient-to-Internal-Observation benefit for two-factor schemes for both factors must be malware-infected for the attack to work. If infecting only one factor breaks the scheme, we don't grant the benefit.

Resilient-to-Leaks-from-Other-Verifiers: This benefit counters the attacks from insiders who leak the information about user passwords or personal information. This makes an attacker to pretend as a valid user to get access to the system resources. This penalizes schemes where insider fraud at one provider, or a successful attack on one back-end, endangers the user's accounts at other sites.

Resilient-to-Phishing: This benefit offers mutual authentication to both user and system. User can communicate with real verifier , server and a victim verifier designed by an attacker who simulates a valid verifier (including by DNS manipulation) cannot collect credentials that can later be used to impersonate the user to the real verifier.

This benefit is not offered by schemes which are vulnerable to more advanced real-time man-in-the-middle or relay attacks.

Resilient-to-Theft: If the scheme uses a physical token or object for authentication, the object cannot be used for authentication by another person who gains possession of it. This benefit offers by the schemes which are resistant to Identity Theft.

We grant Quasi-Resilient-to- Theft, if the protection achieved with the modest strength of a PIN, even if attempts are not rate controlled, because the attack doesn't easily scale too many victims.

No-Trusted-Third-Party: if the scheme does not rely on a trusted third-party (other than the user's and the verifier) who could, upon being attacked or otherwise becoming untrustworthy, compromise the user's security or privacy then this benefit is offers. Most of remote user authentication methods designed either with TTP or without TTP.

Requiring-Explicit-Consent: If user authenticated to a system or resource without his or her consent or user's knowledge then the scheme doesn't offer this benefit. User authentication must start with user's knowledge. This is both a security and a privacy feature. For example, a rogue wireless RFID-based credit card reader embedded in a sofa might charge a card without user knowledge or consent.

Unlinkable: If the user authentication method linked with different user accounts then the scheme doesn't offer Unlinkable service. Colluding verifiers cannot find, from the authenticator alone, whether the same user is authenticating to both. This is a privacy feature. To rate this benefit we disregard linkability introduced by other mechanisms such as same user ID, IP address etc.

We have compared and analyzed user authentication methods for security benefits by giving the ranking and shown in given figure 5.

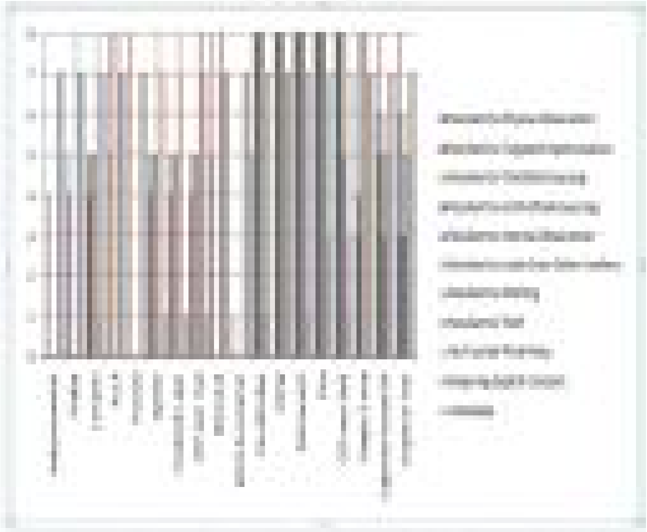


Fig 5: Security benefits of various user authentication methods.

The security benefits for graphical text password as similar to graphical password [2][4]. Graphical text password resistant to both offline and online guessing attacks because of unavailability of password dictionaries for both regional script and graphical elements stored in the database. It is also resistant to both dictionary and brute-force attacks.

V. CONCLUSION

This paper focuses on the security and usability and deployability benefits for various user authentication methods using text, graphical and hybrid passwords. This paper also analyzes the Graphical Text Password, which depends purely on graphical passwords and made user's persuasion to remember letters of telugu or any other language and improve usability of user without compromising the security and deployability benefits. This scheme is also used for both commercial and banking applications through remote user authentication methods.

ACKNOWLEDGMENT

Our sincere thanks to Usability Security Lab (RPC-AICTE Grant) at JNTU Anantapur and the users who involved in survey on user's persuasion to remember the passwords with different user authentication methods.

REFERENCES

1. G.E. Blonder " Graphical passwords": patent in 1999.
2. Raj Mohammed,C.Shoba Bindu " A Novel Cognition based graphical authentication scheme resistant to Shoulder-surfing attack". ICIP'08.
3. Sobrado, L. and Birget, J.C. Graphical passwords. The Rutgers Scholar, 4,(Sept.2002).http://RutgersScholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm
4. Raj Mohammed, C Shoba Bindu, Vasumathi " An Improved Cognition based Authentication Scheme Using PassScript" IJARCS-2011.
5. Divyans Mahansaria et al "A Fast and Secure Solution[SS7.0] that counters Shoulder-surfing attack" Proceedings of the 13th IASTED International conference Software Engineering and Applications(SEA-2009),Cambridge, MA. USA.
6. Dhamija, R. and Perrig, A. Déjà Vu: User study using images for authentication. In Ninth Usenix Security Symposium, 2000.
7. Alain Forget et. al " Improving Text Passwords Through Persuasion" Proceedings of 4 th symposium on Usable Privacy and Security(SOUPS'08).
8. Joseph Bonneau et. al "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" proceedings of the 2012 IEEE Symposium on Security and Privacy.
9. S. Wiedenbeck, J. Waters, J. C. Birget "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme" AVI '06, May 23-26, 2006, Venezia, Italy.Copyright 2006 ACM 1-59593-353- 0/06/0005.
10. S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords." in ACM Computer and Communications Security (CCS), November 2009.
11. M Misbah uddin "A Texto graphic password based authentication scheme" Thesis chapter 5 available at shodaganga. shodhganga.inflibnet.ac.in:8080/jspui/bitstream/.../12_chapter%205.pdf