International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Using PBKDF2 Pair & Hybrid technique for Authentication

Priyanka S. Kedar, Vrunda Bhusari
Computer Department (Pune University)
India

Abstract –

Number of users used the text password scheme for authenticated user. This scheme is used to information security. User is used to authentication by entering the user name and password. Authentication technique is the process of identifying the user based on user name and password. Enter passwords are susceptible to intruders, social engineering, dictionary attacks, shoulder surfing. There are number of problems for text password scheme so, the graphical password is introduced. But also in graphical password, it has a shoulder surfing problem. After the graphical password, in another technique a new password is created by combination of text with image or colors for authentication. PDA is the application of this technique.

Index Terms— Authentication, Dictionary attack, PDA- Personal digital assistant, Session password, Shoulder surfing.

I. INTRODUCTION

Recently there are number of methods used for authentication and security for passwords. Password based user authentication can resist brute force and dictionary attack, when user select strong password for encryption. Textual password authentication method is a traditional method. But normally user select a simple password because they can be easily memorized and can be recalled at login time. Simple password and short password is easy to remembered but it can be easily hacked, while random and lengthy passwords are secured but hard to remember.

To overcome this problem graphical schemes were used. But for graphical authentication scheme it had many problems like shoulder surfing attack. So there are many authentication schemes were proposed to overcome the shoulder scheme attack. But for textual password there are dictionary attacks, shoulder surfing, brute force, social attacks and also in graphical password and biometrics methods are having different disadvantages. In biometric technology there are number of methods such as finger print, iris scan, signature, facial recognition. Disadvantages of biometric scheme is that this system can be costly. In graphical password there is also problem for shoulder surfing. The user is authenticated using session enter the different password. When the session is over then that password becomes is of no use for next session and current session gets terminated. Session password provides more security as every time the session start a new password is created. PDA is personal digital assistant which is application for this system. PDA is used to store confidential and personal data like PIN no., password. There are 3 main categories for authentication technology that are token based, biometric based and knowledge based authentication.. knowledge based authentication method is used for authentication which include both text and picture based password.

II. LITERATURE SURVEY

Dhamjia & perrig[2] proposed a graphical authentication scheme as shown in Fig. 1 . At the time of Registration user has to select number of images from set of random pictures. After at the time of Login, user has to identify the images that pr-selected at the time of registration. This system is susceptible to shoulder surfing.

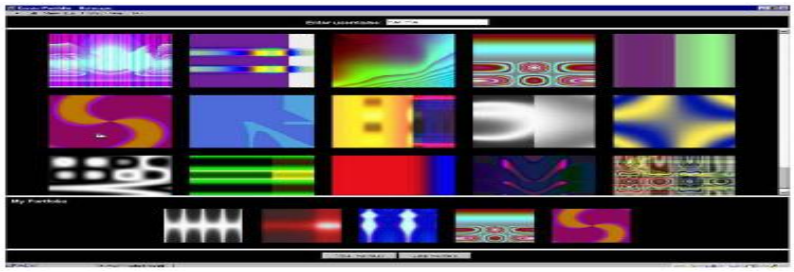

Fig. 1 Images used by Dhamjia & perrig

Syukri[3] developed a new authentication scheme by user drawing the signature using mouse as shown in Fig. 2. This technique uses the two stages, registration and verification.

During the registration stages the user draw his signature with a mouse. System extract the signature area after drawing the signature. In verification stage system takes the input of user signature and extract the parameters of the signature, which draw at the time of registration stage

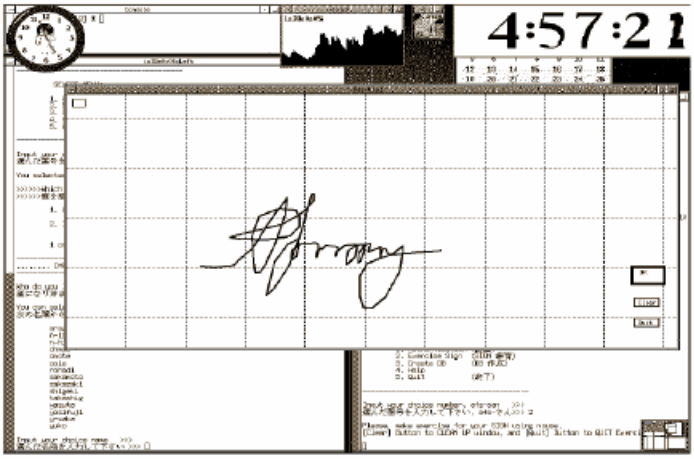

Fig. 2 Signature technique by Sukri

Jermyn[4] introduced a authentication technique called as " Draw_a_Secret"(DAS) as shown in Fig. 3.
In this technique user has to draw the signature by using mouse. Here user is needed to redraw the secret picture on a grid & if that drawing signature touches the same sequence that means user is authenticated person. This technique is vulnerable to shoulder surfing.

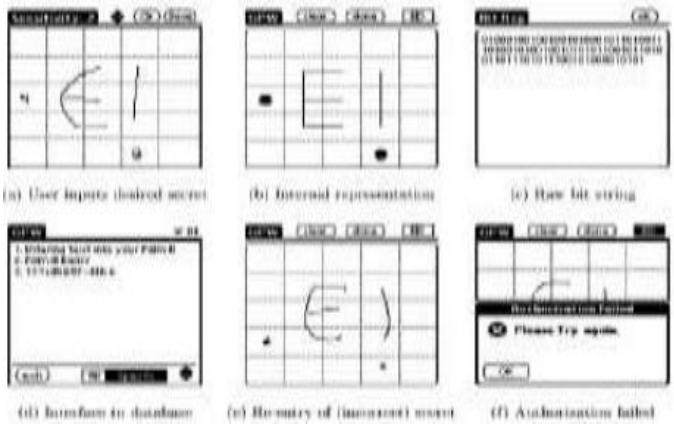

Fig. 3 DAS technique by Jermyn

Wiedenback[5] introduced a graphical password scheme because there are number of problems on shoulder surfing. In this technique user has to remember pass object & click in the convex hull formed of the pass objects as shown in Fig.4.

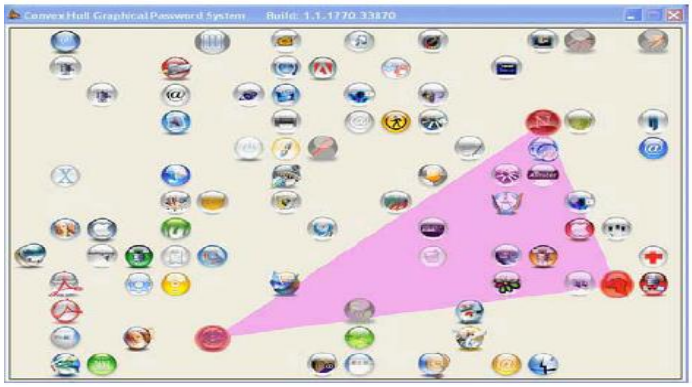

Fig. 4 Example of convex hull

Haichang[6] described a new shoulder surfing resistant technique. As shown in the Fig. 5 here user is needed to draw a curve across the password images orderly rather than clicking on them directly because to confuse to attacker.

Fig 5 Shoulder surfing technique

III. DETAILS OF DISSERTATION WORK

3.1 Platform

Java is the platform of my project

Installation to be done

1. Install the JDK 1.7
2. Install the eclipse IDE
3. Install the MySql Server
4. Install MysqlGuiTool
5. Java Programming Language
6. Windows XP, Windows 7

New Authentication schemes

Authentication technique consists of 3 phases as shown in fig. 6: registration phase, login phase and admin phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

Fig. 6 Authentication scheme

3.1 Admin Phase

In adimn phase administrator can see the on line users and can see the user's information. Only has authority to see the information. He enter th user name and password to see the user information as shown in fig 7

Fig.7 Admin phase

3.2 Registratioin Phase

In this phase if the user is not registered then first he can register his information as shown in fig. 8
As shown in fig.8 user can enter user name,mobile number, first name, last name, email-id and choose the color code as secret password used for Hybrid based technique and submit the information.

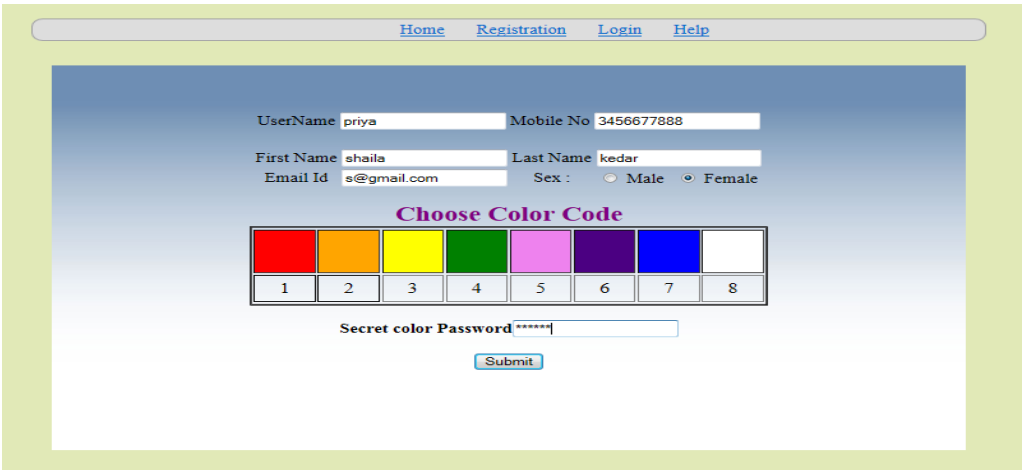

Fig.8 Registration phase

3.3 Login Phase

After registration user can login, user got his password on his email-id and his mobile number . In login user enter his user name and user id as shown in fig.9

Fig.9 Login phase

After login two technologied displayed on the screen for user. User can select any technique for login. Ther are two techniques, one Pair based technique and another Hybrid based technique as shown in fig. 10

Fig. 10 Two authentication schemes

3.4 Pair-Based authentication scheme

At the time of registration user submit his password and minimum length of password character is 8 and it should contain even numbers is called as secret pass[8][9]. By using secret pass session password is generated. At the time of login phase user enter his username and the grid is displayed. The grid size of 8x8 and it consist of alphabets, Special characters and numbers. At any session that are placed randomly on the grid.

Depending upon the secret pass, the password entered by the user. Pair of secret pass has to consider by user so session password consist of alphabets, special characters and digits.

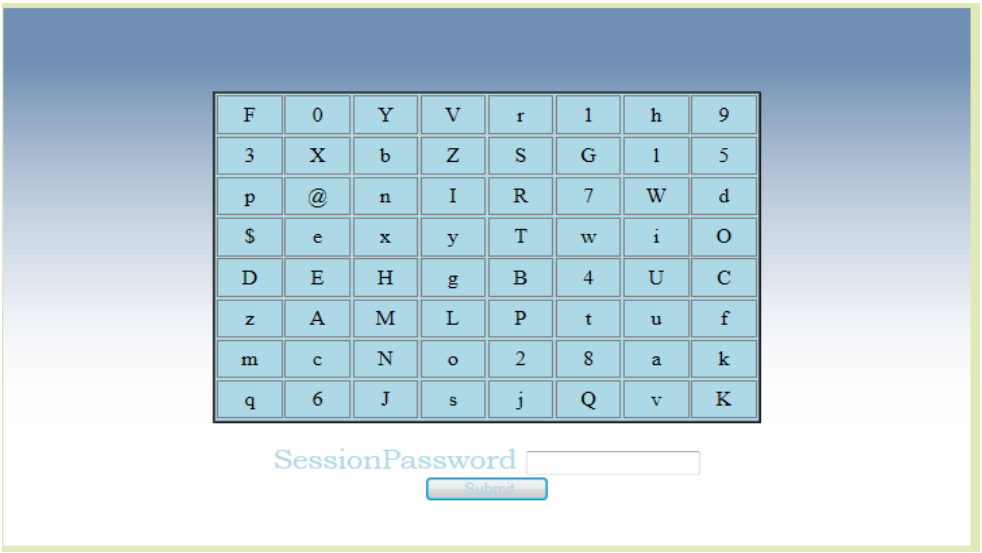

Fig.11 Login Grid with Intersection character

For secret pass user has to consider the password in terms of pairs. From the pair, user has to select the 1st letter from the row and 2nd letter from the column. Select the intersection point of the row and the column , this is the part of the session pass. In this way repeat this procedure for all the pairs of session pass. When user enter the password that is verified by the server to authenticate the user. If the password is valid then n users are authenticated and enter in to the system. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 12 shows that J is the intersection symbol for the pair "Yb". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password

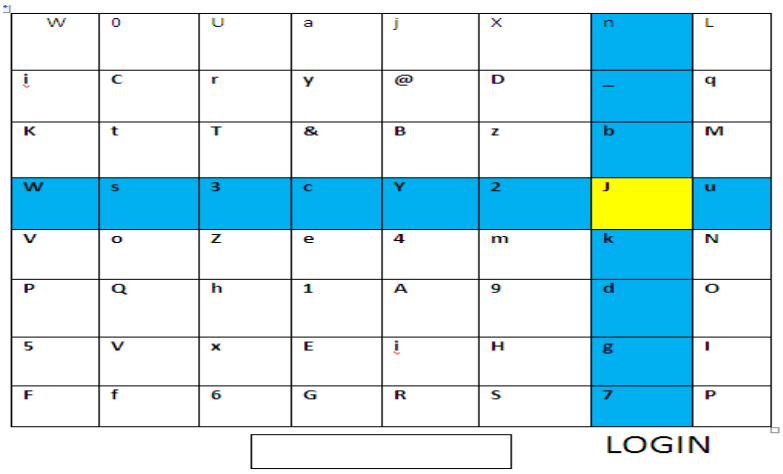

Fig.12 Pair-based intersection grid

After login in pair based technique this screen is displayed on user side. It means user can change the password. He can see his information, add some information and then log out from pair based technique as shown in fig 13

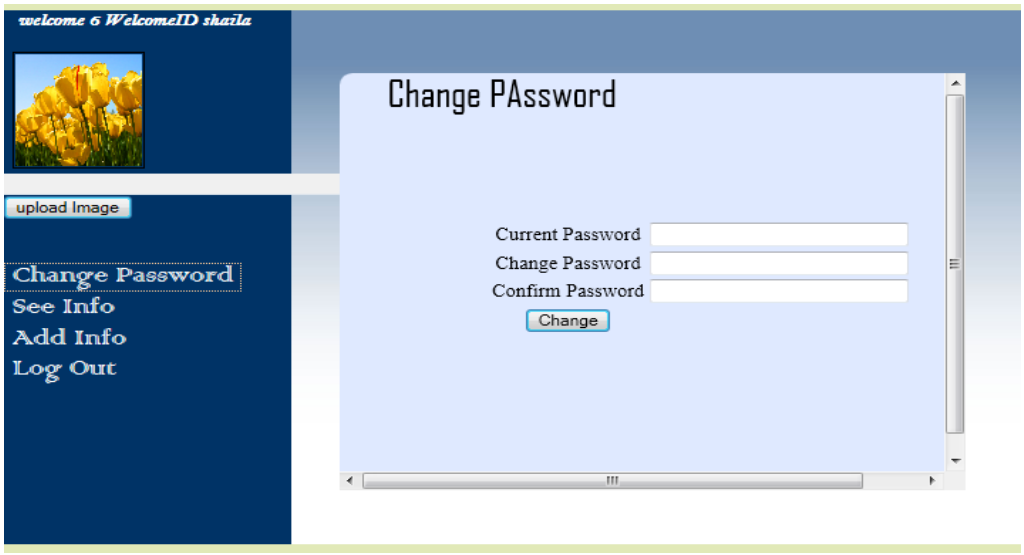

Fig. 13 After login in pair based technique

3.5 Hybrid Textual Authentication Schemes

During registration, user should rate colors as shown in figure. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure. The color grid consists of 4 pairs of colors Each pair of color represents the row and the column of the grid. In Fig. 14 Shows the login interface having the colors grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colours, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure ratings and figure login interfaces for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e 3. The same method is followed for other pairs of colors. For figure the password is "3573**"**. Instead of digits , alphabets can be used.

For every login, both the number grid and the color grid get randomizes so the session password changes for every session. Same method is followed for other pairs of colors. For figure the password is "3573". Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

Fig. 14 Hybrid textual scheme

3.6 SECURITY ANALYSIS

As the interface changes every time the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

- ***Dictionary Attack:***
  These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

- ***Shoulder Surfing:***
  These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session. In hybrid textual scheme, the randomized colors hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of colors. Even by knowing session password, the complexity is 8^4. So these are resistant to shoulder surfing.

- ***Guessing:***
  Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36^4.If the general order is followed for the colors by the user , then there is a possibility of breaking the system.

- ***Brute force attack:***
  These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

- ***Complexity:***
  The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 64^8. In the case of the Hybrid Textual Authentication Scheme the complexity depends on colors and ratings. The complexity is 8! If ratings are unique, otherwise it is 8^8.

3.7 PBKDF2

PBKDF2 is a "password-strengthening algorithm" that makes it difficult for a computer to check that any one password is the correct master password during a brute-force attack

PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0, also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long.

PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a *derived key*, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of

iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

Key derivation function

The PBKDF2 key derivation function has five input parameters:

DK = PBKDF2(PRF, Password, Salt, c, dkLen)

where: *PRF* is a pseudorandom function of two parameters with output length *hLen* (e.g. a keyed HMAC)

Password is the master password from which a derived key is generated

Salt is a cryptographic salt. The standard recommends a salt length of at least 64 bits

c is the number of iterations desired

dkLen is the desired length of the derived key

DK is the generated derived key

Each *hLen*-bit block T_i of derived key DK, is computed as follows:

$DK = T_1 \| T_2 \| ... \| T_{dklen/hlen}$

$T_i = F(Password, Salt, Iterations, i)$

The function *F* is the xor (^) of *c* iterations of chained PRFs. The first iteration of PRF uses *Password* as the PRF key and *Salt* concatenated with *i* encoded as a big-endian 32-bit integer. (Note that *i* is a 1-based index.) Subsequent iterations of PRF use *Password* as the PRF key and the output of the previous PRF computation as the salt:

$F(Password, Salt, Iterations, i) = U_1 \wedge U_2 \wedge ... \wedge U_c$

Where

$U_1 = PRF(Password, Salt \| INT\_msb(i))$

$U_2 = PRF(Password, U_1)$

$U_c = PRF(Password, U_{c-1})$

DK=PBKDF2(HMAC−SHA1/AES, passphrase,ssid,4096, 256)

A key derivation function is useful when encrypting data based on a password or any other not-fully-random data. It uses a pseudorandom function to derive a secure encryption key based on the password

3.8 Comparison with similar systems

Authentication schemes	**Textual password**	**Graphical Password**	Biometric Password	**Session** assword echnique(P/H)
Usability	very high	High	Less	Very High
Implementation	Easy	Complicated	highly complicated	Easy
Attacks	Bruteforce, dictionary, guessing	shoulder surfing, guessing	Forgery	Some times shoulder s rfing
Password space	quite less	Less	no matter	less
Cost of attacks	Low	Moderate	Very High	Low
Time to login	Low	Moderate	High	Moderate
Class	what user remember	what user remember/ recognize	what user is	what user remember
Hardware	not required	not required	Required	Required m bile

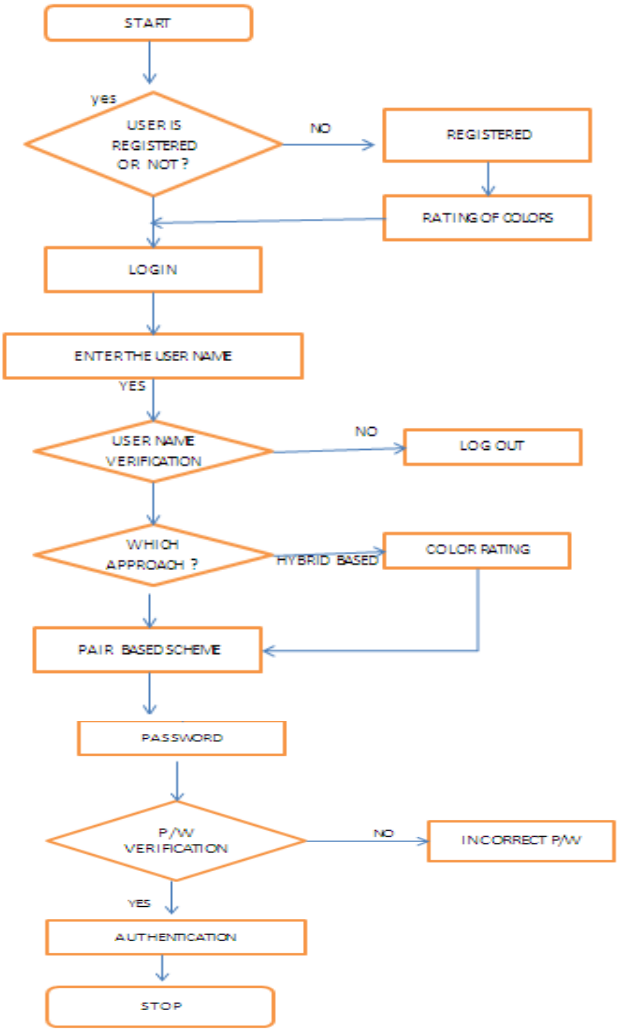

Fig. 15 working of proposed system

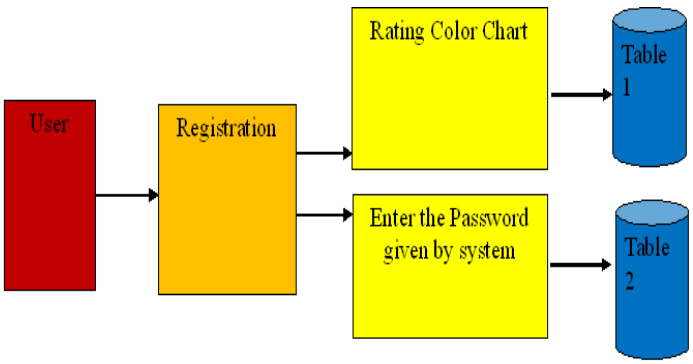

Fig. 16 System Architecture

4. Conclusion and Future Scope

These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. This technique used grid for session password generation. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensive. This technique can be used to develop any windows application or external authentication to connect the application to a database. PBKDF2 can be used for cryptography of session password.

ACKNOWLEDGMENT

I would like to thank everyone, who ever remain a source of help and inspiration for this presentation.

References

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[2] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[3] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[4] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

[6] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing".

[7] Real User Corporation: Passfaces. www.passfaces.com

[8] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "Authentication Techniques For Engendering Session Passwords With Colors And Text" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[9] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May2011

[10] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[11] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[12] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[13] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.

[14] Tejaswi Lalitha Surepeddi, K. Gowtham, A. Ramakrishna,

[15] D. Aruna Kumari, Design, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.1, no.2, pp.44-48, 2012.