International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

USER AUTHENTICATION USING NATIVE LANGUAGE PASSWORDS

Sreelatha Malempati
Dept. of Computer Science & Engineering R.V.R. & J.C. College of Engineering
Chowdavaram, Guntur, A.P
lathamoturi@rediffmail.com

Shashi Mogalla
Dept. of Computer Science & System Engineering Andhra University College of Engineering Visakhapatnam, A.P.
smogalla@yahoo.com

ABSTRACT

Information security is necessary for any organization. Intrusion prevention is the basic level of security which requires user authentication. User can be authenticated to a machine by passwords. Traditional textual passwords are vulnerable to many attacks. Graphical passwords are introduced as alternatives to textual passwords to overcome these problems. This paper introduces native language passwords for authentication. Native language character set consists of characters with single or multiple strokes. User can select one (or more) character(s) for his password. The shape and strokes of the characters are used for authentication.

KEYWORDS

Shape based authentication, Textual Password, Native language password, Intrusion prevention

1. INTRODUCTION

The main objective of the intruder is to gain access to a system with the knowledge of some user's password and login to a system like a legitimate user. The first step of defense against intruders is the password system. In all multi-user systems, user provides login ID and password which serves to authenticate the user. Generally users select a password that is too short or too easy to guess. The password length and the guessable passwords are two main problems in password protection. When users select a password that is guessable such as their first name, birthday, mobile number, child's name, vehicle number, favorite actor and so forth, the password cracking is straight forward. If the password length is too short, it is easy for intruder to find the password. If users select long passwords, it would be difficult for most of the users to remember their passwords. Users select English for their textual passwords and it makes password guessing, eaves dropping, dictionary attacks and shoulder surfing easy. To overcome these vulnerabilities, graphical password schemes have been introduced.

The graphical password schemes use images or shapes for authenticating the user. Users remember the images or shapes better than textual password. But for graphical schemes, shoulder surfing and hidden cameras are the main problems. As an alternative to textual passwords, biometrics, such as finger prints, iris scan or facial recognition have been

DOI : 10.5121/ijnsa.2011.3611

introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. More over this approach requires a special sensor for the biometric. In this paper, a new shape based textual authentication scheme for native language passwords is proposed. Users can remember their native language passwords better than any other language. User selects a character from his native language and submits the shape of that character in a grid during password creation. Later based on this information, the user is authenticated.

This paper is organized as follows: Related work is discussed in section 2, in section 3 the new shape based textual authentication scheme is introduced, Security analysis is done in section 4, user study is given in section 5 and conclusion is proposed in section 5.

2. RELATED WORK

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text. There exist various approaches that focus on graphical authentication schemes. Blonder [1] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of the locations. Dhamija and perrig [2] proposed a graphical authentication scheme in which the user selects a certain number of images from a set of random pictures. Later user has to identify the pre-selected images for authentication. Jansen [4,5] proposed a graphical password scheme for mobile devices. During password creation, the user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the no. of images is limited to 30, the password space of this scheme is not large. Weinshall and Kirkpatrick [10] proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes. Goldberg [3] designed a technique known as “pass doodle”. This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen. Jermyn et al [6] proposed a technique called “ Draw A Secret”(DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order. All these graphical authentication schemes are vulnerable to shoulder surfing.

To overcome the shoulder-surfing problem, many techniques were proposed. Zhao and Li [12] proposed a shoulder-surfing resistant scheme “S3PAS”. The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al, [8] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass-objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. Luca, et al. [7] proposed a stroke based shape password for ATMs. They argued that using shapes will allow more complex and more secure authentication with a lower cognition load. More graphical password schemes have been

summarized in a recent survey paper [9]. Zheng et al [13] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text. The user has to select a shape which can be a number, character (in English), geometric shape or a random shape. But selecting simple and common shapes makes the process easy for the intruder. Though the random and arbitrary shapes are strong, it is difficult for the user to remember them.

M Sreelatha and M Shashi [9] proposed modified schemes for hybrid authentication technique which is based on shape and text to make it more secure. M Sreelatha et al [10] proposed image based authentication techniques for PDAs. Pair based image authentication technique uses recognition based approach in which user has to recognize his pairs. Text based image authentication uses both recognition and recall based approaches where user has to recognize his images and recall the characters assigned to them. M Sreelatha et al [11] proposed two techniques for generating session passwords for authentication. Text and colors are used to generate session passwords for authentication. These are shoulder-surfing resistant techniques. Sreelatha Malempati and Shashi Mogalla [12] proposed an authentication technique based on well known ancient Indian board game to enhance the memorability, usability and security of passwords. They performed user study as paper work [13] and found that the tool is a promising approach to enhance all aspects of the passwords. Sreelatha malempati and Shashi Mogalla [14] proposed an authentication technique based on native language characters for password. Naturally, users remember their native language passwords better than any other language. The shape and strokes of the native language characters are used for authentication. This paper focuses on user study for time required for registration and login of native language password authentication technique.

3. THE AUTHENTICATION SCHEME

The new shape based textual authentication scheme consists of three steps:

- password creation
- password entry
- password verification

3.1 Password creation

User selects a character from his native language character set. Each character may contain one or more strokes. A stroke is an ordered list of cells. A password is represented by a sequence of strokes. The length of a stroke is the number of cells it contains. The length of the password is the sum of the lengths of its strokes. An interface consisting of a grid of size 5x 5 will be displayed on the screen. User has to select an ordered list of grid cells to represent the shape of the character selected for password. The character “na” in Fig 1 consists of single stroke and it can be represented by the sequence {(4,2),(3,2),(3,3),(4,3),(4,3),(3,3),(2,3),(2,2),(1,3)}. The character “oo” in fig 2 consists of three strokes. The first stroke consists of grid cells {(2,3),(2,2),(3,3),(4,2),(4,3),(4,3)} and the second stroke consists of grid cells {(3,2),(3,3)} and the third stroke consists of {(1,3),(2,3)}. Totally, the character “oo” can be represented by the sequence {(2,3),(2,2),(3,3),(4,2),(4,3),(4,3),(3,2),(3,3),(1,3),(2,3)}

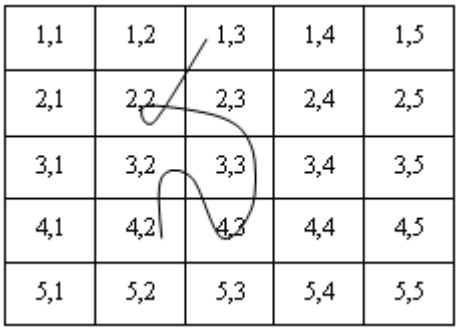


Fig 1: The character "na"

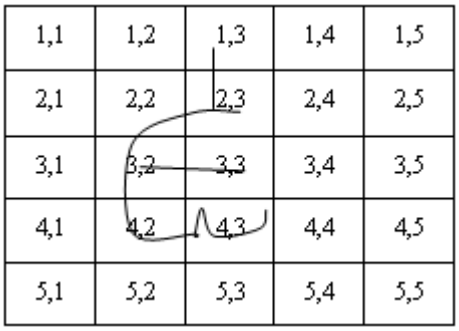
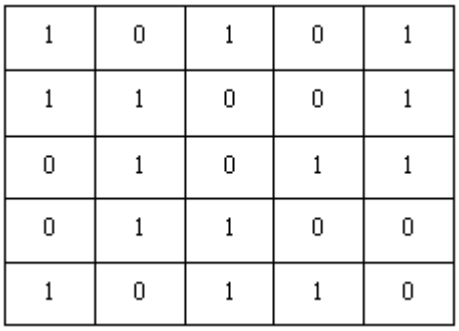


Fig 2: The character "oo"

3.2 Password entry

At the time of login, user has to enter his login ID and password. An interface consisting of grid of size 5x5 will be displayed. The grid contains a symbol in each cell. Based on the symbol in the grid cells and shape of the character selected by him, user has to enter his password.



Login ID: _____
Password: _____

Fig 3: Login interface grid with symbols

For this interface, suppose the user enters the password: **110110011**

3.3 Password verification

After password entry, the authentication scheme verifies the password. It will compare the symbols of the interface in the positions of the grid cells selected by the user at the time of password creation with the symbols of the password entered by the user at the time of login. If the password entered is not correct, the system generates another login interface grid with different symbols. At each login step, the symbols vary, but the shape of the character and the order of the grid cells that represent the shape of the character do not vary and the password entered by the user varies. So, session passwords are generated instead of static passwords.

For the above interface, the password will be verified in this manner:

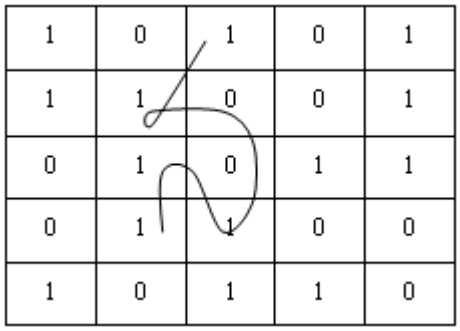


Fig 4: grid with shape of the character

The shape of the character is represented by the cells:
{(4,2),(3,2),(3,3),(4,3),(4,3),(3,3),(2,3),(2,2),(1,3)}
For this interface, by considering the symbols of the cells in the above order, actual password is **110110011**
and the password entered by the user is **110110011.** In this example, system authenticates the user.

4. SECURITY ANALYSIS

4.1 Size of the grid

If the grid size is small, it is easy to enter the password and at the same time it is easy for the intruder to crack the password. With a grid of small size it may not be possible to represent all the characters of the native language properly. If the grid size is large, then it is difficult for the intruder to break the password. Each character can be represented in many ways and it may be difficult for the user to remember the position of the grid cells. Grid size should be moderate to use the system effectively.

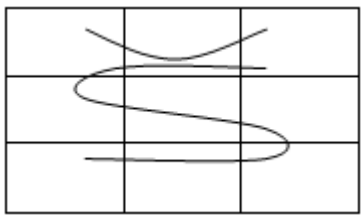


fig 5 : 3x3 grid

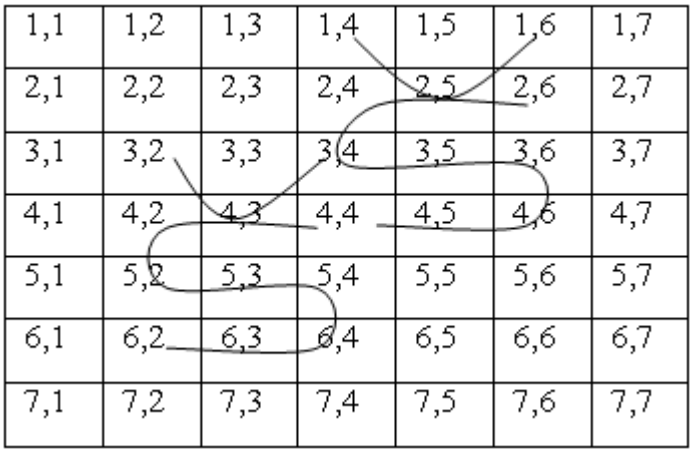


Fig 6: 7x7 grid

4.2 Complexity

In this paper, Telugu language is selected as the native language of the user. Telugu is one of the official languages of India. There are 18 vowels and 36 consonants in the language. A syllabic unit could be a vowel, a consonant or their combination. In a combination, the vowel part is indicated using a diacritic sign known as maatra. The shape of a maatra is often completely different from the corresponding vowel. The shape of the consonant also changes when it combines with a vowel or with another consonant. Each character is represented by one or more strokes with some strokes extending above or below the main part of the character. There may be overlapping of these strokes in many of the characters. This overlapping of strokes leads to repetition of grid cells in the password creation.

The grid consists of 3 types of cells - internal cells, boundary cells and corner cells. An internal cell of the grid consists of 8 neighbors, a boundary cell consists of 5 neighbors and a corner cell consists of 3 neighbors. The actual complexity depends on the type of cells selected by the user for his password. For simplicity, we are considering that all selected cells are internal cells.

Case 1: The character contains a single stroke:

Suppose the shape of the character selected for password contains n cells.

(a) without repetition of grid cells:
Theoretically, the password space is 25*24*23* …(25-(n-1)) .
But, practically it is less than that value. Every cell in the stroke (except the first cell) is a neighbor of the previous cell. After selection of the first cell with 25 possibilities, the no. of possibilities of selection of the second cell is 8 and third cell is (8-1). The total password space is 25 * 8 * 7 ^ (n-2).

(b) With repetition of grid cells, theoretically the no. of possibilities is 25 ^ n. practically the password space is 25 * 8 ^ (n-1).

Case 2: The character contains two or more strokes

(a) Without repetition of grid cells:

If there are two strokes with n and m symbols then the password space is 25 * 8 * 7 ^ (n-2) of the first stroke and (25-n) * 8* 7 ^ (m-2) for the second component for internal cells.

(b) With repetition of grid cells

With repetition, the password space is 25 * 8 ^ (n-1) of the first stroke and 25 * 8 ^ (m-1) of the second stroke. With more no. of components, it will be more difficult to crack the password.

4.3 Shoulder surfing

These attacks do not work with the proposed shape based textual authentication scheme even though intruder has a copy of the password entered by the authenticated user. Every time the symbols of the login interface grid changes and the password varies. Suppose that the intruder has obtained the interface grid and the password entered during login step. The intruder has to guess the shape of the password based on strokes. A single password represents many stroke variants. The total password space depends on number of 1's and 0's in the interface grid and the password entered. Suppose, the interface grid consists of m number of 1's and n number of 0's and the password consists of p number of 1's and q number of 0's. The password space is (m ^ p) * (n ^ q).

4.4 Random input

The possible symbols for the password are {0,1}. By giving random input, the possibility of guessing the correct password of length k is (1/2) ^ k = 1 / (2 ^ k).

4.5 Eaves dropping

Password may be accessed by unauthorized users during transmission from client to server. Encryption is the common method used for avoiding unauthorized access. It is computationally expensive. Using native language password authentication, the grid data and the password entered are transmitted to the server. If the intruder captures both grid data and the password entered by the user, he cannot get the sequence of the password directly. He has to try all possible alternatives in order to get the shape of the character which is equivalent to shoulder-surfing attack.

The complexity of detecting the password sequence depends on the number of strokes involved, total length of the password sequence and reusing the grid cells. There is no restriction on the length of the password but, practically it is difficult to enter long password for every login.

4.5 Hidden camera

Suppose the intruder has a copy of the login interface grid and the password entered by the authenticated user captured by hidden cameras. For the login interface grid in fig:3, the password entered by the user is **110110011**. When the intruder tries to find the character of the password, he may find many characters of the language as shown below from fig 7 to fig 12.

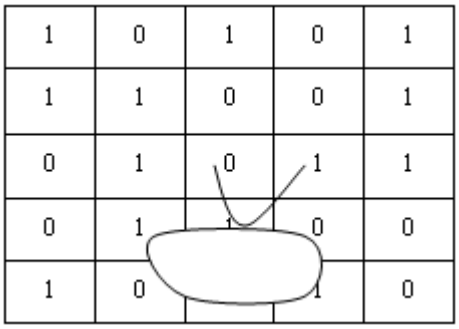


Fig 7: the letter “ra”

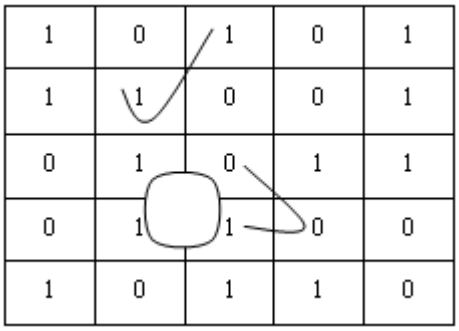


Fig 8: the letter “pa”

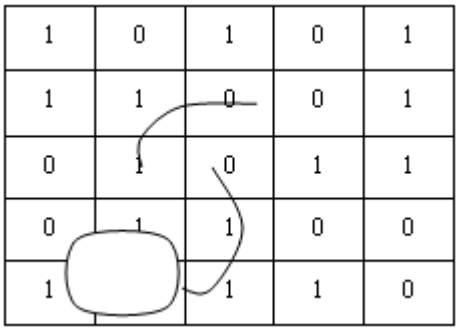


Fig 9: the letter “ea”

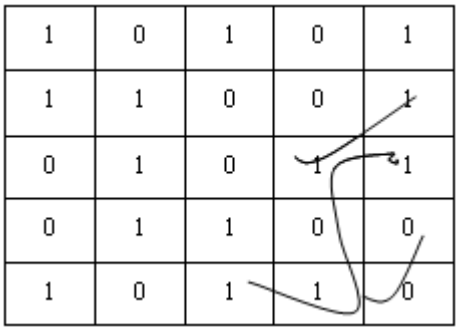


Fig 10: the letter “ku”

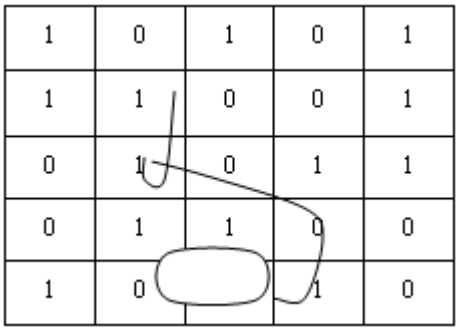


Fig 11: the letter “va”

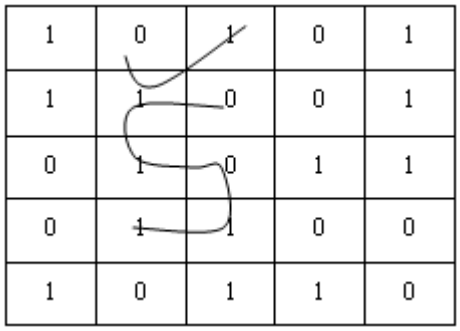


Fig 12: the letter “ka”

With the same password, the login interface grid may represent number characters of the language. Even though generally the strokes of the language go from left to right and top to bottom, it may depend upon the writing style of the user. The user takes freedom in selecting characters of the language either by his style or just for the password. For example, in fig 12, the first component of the letter “ka” goes from bottom to top. It’s sequence is {(4,2),(4,3),(3,3),(3,2),(2,2),(2,3)} instead of {(2,3),(2,2),(3,2),(3,3),(4,3),(4,2)}.

5. User study

We conducted user study with 20 Second year Engineering students. 10 students selected random shapes as their password and the other 10 students selected Telugu character as their password. We calculated the password registration time and login time for all users. The

students were requested to do registration after a training session. During training session, the proposed authentication technique was explained and the password registration and the login process were demonstrated. Login time is measured for four logins and the average was calculated. The registration time and login time for simple passwords are comparatively less than complex passwords. Most of the native language password characters contain more number of grid cells. Because of the shape of the characters and number of cells required for the characters, these characters took more time for registration and login than the random shapes.

Table 1 : Random shapes as passwords

User	Registration time	Login time
User1	4.6725	6.1433
User2	7.1690	9.0298
User3	7.9540	9.5120
User4	10.0605	9.3278
User5	9.0250	9.5275
User6	7.2045	8.2735
User7	11.5435	11.9603
User8	10.3675	10.8912
User9	11.375	11.9188
User10	9.9920	9.8828

Table 2: Native language characters as passwords

User	Registration time	Login time
Usert1	9.4445	11.1150
Usert2	7.6090	9.5988
Usert3	9.1705	12.0894
Usert4	7.3660	9.4630
Usert5	10.2340	10.0964
Usert6	9.1085	9.7708
Usert7	8.7570	10.9033
Usert8	12.4840	11.8740
Usert9	10.5085	12.5156
Usert10	10.0155	10.8353

We conducted memorability test for the students after first week and second week of registration by considering two points. First point is remembering the password and the second point is successful login. All the users are able to remember their native language password character but all of them were not successful in login. The reason is they were not able to remember the sequence of grid cells properly. In the case of random shapes, some of the students who selected random shape as password were not able to remember the shape. This indicates that the users are able to remember the native language characters better than random shapes, but, the usability of passwords should be improved. Native language character set should be simplified in order to increase the usability and security of passwords.

Table 3 : Random shapes and Native language character passwords

username	Cell1	Cell2	Cell3	Cell4	Cell5	Cell6	Cell7	Cell8	Cell9	Cell10	Cell11	Cell12
user1	(1,1)	(5,1)	(5,5)	(1,5)	(3,3)	null	null	null	null	null	null	null
user2	(1,1)	(1,2)	(5,5)	(5,4)	null	null	null	null	null	null	null	null
user3	(1,1)	(2,2)	(1,5)	(2,4)	(5,1)	(4,2)	(5,5)	(4,4)	null	null	null	null
user4	(2,2)	(3,2)	(4,2)	(3,3)	(4,4)	(3,4)	(2,4)	null	null	null	null	null
user5	(2,3)	(2,2)	(3,2)	(4,2)	(4,3)	(4,4)	(3,4)	(2,4)	null	null	null	null
user6	(4,1)	(5,2)	(5,2)	(4,3)	(3,4)	(2,5)	null	null	null	null	null	null
user7	(1,2)	(2,2)	(3,2)	(4,2)	(5,2)	(3,2)	(2,3)	(1,4)	(3,2)	(4,3)	(5,4)	null
user8	(4,5)	(4,4)	(4,3)	(4,2)	(3,3)	(2,4)	(3,4)	(4,4)	(5,4)	null	null	null
user9	(4,1)	(3,2)	(2,3)	(2,4)	(2,5)	(4,5)	(4,4)	(4,3)	(3,2)	(2,1)	null	null
user10	(2,3)	(3,2)	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(3,4)	null	null	null	null
usert1	(2,4)	(2,3)	(2,2)	(3,2)	(3,3)	(3,4)	(4,4)	(4,3)	(4,2)	(1,2)	(2,3)	(1,4)
usert2	(4,2)	(3,2)	(2,3)	(3,4)	(4,4)	(1,2)	(2,3)	(1,4)	null	null	null	null
usert3	(2,3)	(2,2)	(3,2)	(4,2)	(4,3)	(4,4)	(3,4)	(2,4)	(1,2)	(2,3)	(1,4)	null
usert4	(5,2)	(4,2)	(4,3)	(5,3)	(5,4)	(4,4)	(2,2)	(3,3)	(2,4)	null	null	null
usert5	(3,2)	(3,3)	(2,3)	(2,2)	(3,2)	(4,2)	(4,3)	(4,4)	(3,4)	(2,4)	null	null
usert6	(2,1)	(2,2)	(2,3)	(3,3)	(4,3)	(4,2)	(4,2)	(4,3)	null	null	null	null
usert7	(5,2)	(4,2)	(4,3)	(5,3)	(5,4)	(4,4)	(3,4)	(3,3)	(3,3)	(2,4)	null	null
usert8	(2,3)	(2,2)	(3,2)	(4,2)	(4,3)	(4,4)	(3,2)	(3,3)	(1,3)	(2,3)	null	null
usert9	(3,2)	(3,1)	(4,1)	(4,2)	(4,3)	(3,3)	(4,4)	(3,4)	(2,3)	(3,3)	(2,4)	Null
usert10	(4,2)	(4,1)	(5,1)	(5,2)	(5,3)	(4,3)	(2,1)	(3,2)	(2,3)	null	null	null

Table 4: Memorability Test

	Type of password	Password remembered	Login successful
After First week	Random shapes	8	7
	Native language characters	10	7
After Second week	Random shapes	7	6
	Native language characters	10	5

6. CONCLUSION

In this paper a new authentication scheme based on native language passwords is proposed. In this paper, Telugu language is selected as the native language of the user. Telugu is one of the official languages of India. The proposed scheme is resistant to eves dropping, brute force attack, shoulder surfing and hidden camera. Users can remember their native language passwords better than any other language. The intruder should have the knowledge of native language of the user to guess the password to break the system. During registration, user selects sequence of cells on the grid based on the shape of the character selected by him for password. For login, user has to enter the symbols in the grid in the same sequence selected by him during registration. By user study, it is observed that the native language character passwords are taking more registration time and login time. Though users are able to remember their character, they are not able to remember the shape of the pass word properly. The native language character set should be simplified to overcome these problems, which is future work for this paper.

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, "Deja Vu: A User Study using Images For Authentication", 9th USENIX Security Symposium, 2000.

[3] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[4] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.

[5] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[6] 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.

[7] A. D. Luca, R. Weiss, and H. Hussmann, "PassShape:stroke based shape passwords," in *Proceedings of the conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments*. 28-30 November 2007, Adelaide, Australia, pp. 239-240.

[8] S.Man, D. Hong, and M.Mathews, "A shouldersurfing resistant graphical password scheme," in *Proceedings of International conference on security and management. LasVergas*, NV, 2003

[9] M Sreelatha, M Shashi , " Modified schemes for authentication based on shape and text " International Journal of Electrical, Electronics and Computer Systems IJEECS, volume 1, issue 2, April 2011

[10] M Sreelatha, M Shashi , M Roop Teja, M Rajashekar, K Sasank " Intrusion Prevention by Image Based Authentication Techniques " in the proceedings of IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, MIT, Anna University, Chennai, June 3-5, 2011, pp. 1239-1244

[11] 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 and It's Applications, IJNSA, Vol 3, No. 3, May 2011, DOI : 10.5121/ijnsa.2011.3308

[12] Sreelatha Malempati, Shashi Mogalla, "A Well Known Tool Based Graphical Authentication Technique", in proceedings of the conference CCSEA 2011, CS & IT 02, pp. 97-104, DOI: 10.5121/csit.2011.1211

[13] Sreelatha Malempati, Shashi Mogalla, " An Ancient Indian Board Game as a Tool for Authentication" International journal of Network Security and It's Applications, IJNSA ,Vol 3, No. 4, July 2011, pp.154-163, DOI : 10.5121/ijnsa.2011.3414

[14] Sreelatha Malempati, Shashi Mogalla, "Intrusion Prevention by Native Language Password Authentication Scheme" in the proceedings of 4th International Conference, CNSA 2011, CCIS 196, pp. 239-248, Springer-verlag Berlin Heidelberg 2011

[15] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," *21st Annual Computer Security Applications Conference (ASCSAC 2005)*. Tucson, 2005.

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

[17] William Stallings "Cryptography and Network Security", 4th Edition. Publisher – Pearson Education Inc.

[18] 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.

[19] 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.