e-ISSN: 2349-9745
p-ISSN: 2393-8161
6FLHQWLILF -RXUQDO ,PSDFW)DFWRU 6-
,QWHUQDWLRQDO -RXUQDO RI 0RGHUQ 7
DQG 5HVHDUFK
ZZZ LMPWHU FRP

Security Enhancement for Databases Using Multifactor Authentication

K. Nandhini[1], T. Narmadha[2], J. Vijayaraj[3],
[1,2,3]Department Of Information Technology,S.K.P. Engineering College, Tiruvannamalai.

Abstract: $XWKHQWLFDWLRQ SODYV D YLWDO UROH LQ DOO WKH
Though various authentication schemes are available to provide security in the databases, data confidentiality is not achieved properly. To face this problem, a technique named, Multifactor Authentication is proposed. Here, authentication is done by clicking images on different locations at various levels to provide the improved security for the user applications, which are more confidential.
Keywords: Multifactor Authentication, Data Confidentiality, Graphical Passwords.

I. INTRODUCTION

Computer systems are most often accessed based on alpha-numeric passwords and these passwords are used in multi-user operating systems for authentication and to solve security issues. But, the alpha-numeric passwords are difficult to remember for a user, when it is long and random appearing. As, there are various possibility for password guessing attack and dictionary attack, these passwords can be captured and reused when the user access the applications in public computers. Hence, the single factor authentication is considered to be an inadequate method for the high risk DSSOLFDWLRQV LQFOXGH DFFHVVLQJ WKH GDWDEDVHV RI confidential information. In order to resolve the problems of single factor authentication, a technique named Multifactor Authentication scheme is used. Multifactor Authentication is the method, in which the text-based authentication is combined with another factor. In this scheme, the sequences of clickable points of selected image at various levels are considered to be passwords. Since, graphical passwords are easy to remember and less resistant to attack, as the search space of image is practically infinite.

II. TECHNIQUES USED

The user clicks the images at various pixels to make them as passwords using the graphical password schemes named recognition and recall-based techniques. There are two methods available for the user and these methods are easy to use as the user has to remember only the images and click points.

In Recognition-based technique, the set of images are provided to the user. The user has to select the images in a correct sequential order. This technique contains several rounds. The user has to select correct images in each round for successful login. During login, the same images from panel are provided, but their locations are changed.

In Recall-based technique, the user has to reproduce something in the manner, in which, the user has selected before during the registration stage.

III. SYSTEM ARCHITECTURE

IV. PROPOSED SYSTEM

There are two methods used in the proposed system for user authentication. The user can select any one of the two methods of their choice.

In both methods, at the registration stage, the user has to provide the email id as user name and then the password should be entered.

Method 1:

In the first method, at the registration stage, when the user provides the user name and password, the authentication server provides the image portfolio, which contain group of images from the image panel are displayed. The user has to select a particular image from the portfolio. Then the user has to click on the particular x and y co-ordinates at various locations of an image at three different levels. The sequences of clickable points in an image are considered as password. Thus, the user details and clicked pixels are stored in the authentication server.

When the user attempts to login the application, the user has to provide user name and password. When the user details match with the logs in the databases of authentication server, the images are provided and the user has to click on the same pixels as passwords and they are again compared with the server. When the clicked points match with the logs, then the OTP is generated and provided to the user. Once, the user enters the valid OTP, the user is authenticated and allowed to access the application.

Method 2:

In the second method also, at the registration stage, when the user provides the user name and password, the group of images are provided by the authentication server to the user. From the portfolio, the user has to select the sequence of images and click on each image of their choice.

Thus, every clicked point on selected image in the sequential order is considered as passwords.

When the user attempts to login, the user has to provide the user name and password. When the user details match with the database, the server provides images and now, the user has to click on the every selected image in the correct order as done in the registration stage. When the clicked points match the log in the server, the OTP is provided to the user and after entering the valid OTP, the authenticated user is allowed to access the application.

In the above two methods, when the user exceeds the level of attempts, the security question is also provided to ensure that the user is a valid person.

V. CONCLUSION

In this paper, we have proposed the simple multifactor authentication scheme that includes two authentication methods, which uses various clickable points of an image as passwords. The user can use any one of the two methods to protect the available information in a better manner. Although, image based authentication schemes are not well known to many user currently, they might have wider applicability in future to enhance the password quality and security, compared to single factor authentication.

REFERENCES

[1]. Alireza Pirayesh Sabzevar, AngelosStavrou, ´Universal Multi-)DFWRU $XWKHQWLFDWLRQ 8VLQJ
Computer Science Department,George Mason University.

[2]. Susan Wiedenbeck Jim Waters, Jean-&DPLOOH %LUJHW $OH[%URGVNL\1DVLU0HPRQ Authentication Using Graphical 3DVVZRUGV´ 'HSDUWPHQW RI &RPSXWHU Science, Rutgers University

[3].SrinathAkula,VeerabhadsramDevisetty ³,PDJH %DVHG 5HJLVWUDWLRQ DQG $XWKHQWL Computer Science, St Cloud State University St. Cloud, MN 56301.

>@ %LQ % =KX -HII <DQ *XDQER%DR 0DRZHL <DQJ ²A New Security 1;X ´ &D 3ULPLWLYH %DVHG RQ +DUG $, 3UREOHPV´ IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[5]. Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny ³$ 3URILFLHQW 0XOWLOHYHO *UDSKLF International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, No 6, June 2013.Pg 1341-1344.

[6]. 0G $VUDIXO+DTXH %DEEDU -RDUH Round Hybrid Password 1HZ $FKHPH´³ ,QWHUQDWLRQD Computer Engineering and Technology (IJCET), Vol. 3, Issue 2, July-September (2012).

[7@ + 7DR DQG &-Go. $ GDPVV A proposal to improve the usability of JUDSKLFDO SDVVZRUGV´ International Journal of NetworkSecurity vol. 7, no. 2, pp. 273 ±292, 2008.

[8]. +DLFKDQJ*DR ;L\DQJ /LX 5X\L 'DL ³'HVLJQ DQG3$QDO\VLV RI D 6FKHPH´ International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 ±678.