IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THREE LEVEL PASSWORD AUTHENTICATION SYSTEM

[1]Dr Prakash Bethapudi, [2]T Harika, [3]G Nirisha, [4]K Prasanna
[1]Professor, [2]B.Tech IV, [3]B.Tech IV, [4]B.Tech IV
[1,2,3,4] Information Technology,
[1,2,3,4] Vignan's Institute of Engineering for Women, Visakhapatnam, India

Abstract: In the present situation security is highly important. Keeping that as a major issue here we form a 3-level security system which increases the confidentially to the password in a higher level. At each session user need to get authenticated so that it is able for them to proceed to the next level. LEVEL 1- **authenticated by OTP generation via email,** LEVEL 2- **authenticated by explicit calculation-based method,** LEVEL 3- **authenticated by image ordering.** After getting authenticated in all the levels the user can use the system. If fails to authenticate in any level then it is not possible to move to the next level

***Index Terms* – Authentication, Security, Confidentiality, Password, OTP**

generation, Image Ordering

I. Introduction

The project is an authentication system that validates user for accessing the system only when they have input correct password. The project involves three levels of user authentication. Short, almost all the passwords available today can be broken to a limit. Hence this project is aimed to achieve the highest security in authenticating users. It contains three logins having three different kinds of password system. The password difficulty increases with each level. Users have to input correct password for successful login. The project comprises of OTP based, virtual password and image ordering for the three levels respectively.

II. Existing System

In existing system Security sensitive environments protect their access control mechanisms against unauthorized access. A 3-level Password authentication system that combines the features of existing authentication schemes. The different levels used in that are **image ordering** which involves selection of different images from an image grid**, colored pixels** which is based on intensity and brightness of the colors **and one-time-password** to provide high level security. Text based passwords are not highly secured so the above are add-ins to it. But For SMS based OTP the mobile needs to be handy so that it is improvised to email. Takes high time for the process of authentication and user need high memorizing Power.

III. Proposed System

In Proposed system as Password authentication should encourage strong security. We propose that authentication schemes allow user choice while influencing users towards strong passwords. We have upgraded the levels to increase performance though it ranges to complexity. Will develop OTP based password authentication via email. Developing one security level of password generation explicitly and also used an image pixel-based method in the stage of three to get authenticated then would definitely make the process easy and at 3 levels we have designed something new and different from the present one making user process easy.

IV. Description and Methodology

Here as it comes over 3 levels, lets discuss the structure of 3 levels individually.

LEVEL1: Here the user gets authenticated via email. The code generates a random OTP at the backend. The OTP is sent to user authenticated mail. User uses this OTP to proceed to level 2 of authentication

1. Backend server generates the secret key
2. The server shares secret key with the service generating the OTP. Since both the server and the device requesting the OTP, have access to time, which is obviously dynamic.
3. The code generated to the desired length suitable for the user to enter.
4. A counter is used to keep track of the time elapsed and generate a new code after a set interval of time. OTP generated is delivered to user with the help of mail that is stored at the backend.

LEVEL2: Here the user will provide a secret string and a password and also selects some of the values in a pre-defined matrix at the time of registration phase and at login phase the string and password need to be concatenated with the help of system generated matrix values.

Here a user needs to select a pass pattern which is in an array form

Pass pattern: X1, X5, X9 followed by 3*3 array
X1 X2 X3
X4 X5 X6
X7 X8 X9

Secret password need to be selected by user (Secret password = "kat")

Secret function need to be selected by the user (Secret function=1)

1. +, -, *

2. -, +, *

3. *, -, +

System generates a random array, user should note this pass pattern values. (System generated value = 2,7,8) from pass pattern array

4. 2 3 4

5. 5 7 9

6. 1 6 8

The user password will be based upon pass pattern values and function applied

7. 1 + 2 = 3 3 - 7 = 4 4 * 8 =32 =3432

8. The final part is to add user secret string with calculated value, which is the virtual password. ("kat" + 3432 = kat3432)

LEVEL3: Users select click points on image. The image is uploaded as soon as a user selects a click point and pixel points are saved for next login authentication. If a user enters a correct click-point during login, then he will be authenticated

1. Intially an image is designed in form of grid with some hidden values over it using java script
2. Then the user needs to select some cluepoints from an image where the values that are present inside it are stored in a textbox
3. The similar process need to be repeated for the second image

Now if the click points match and similar in the textboxes of the images then the authentication is successful else need to repeat the process

V. FLOW DIAGRAM:

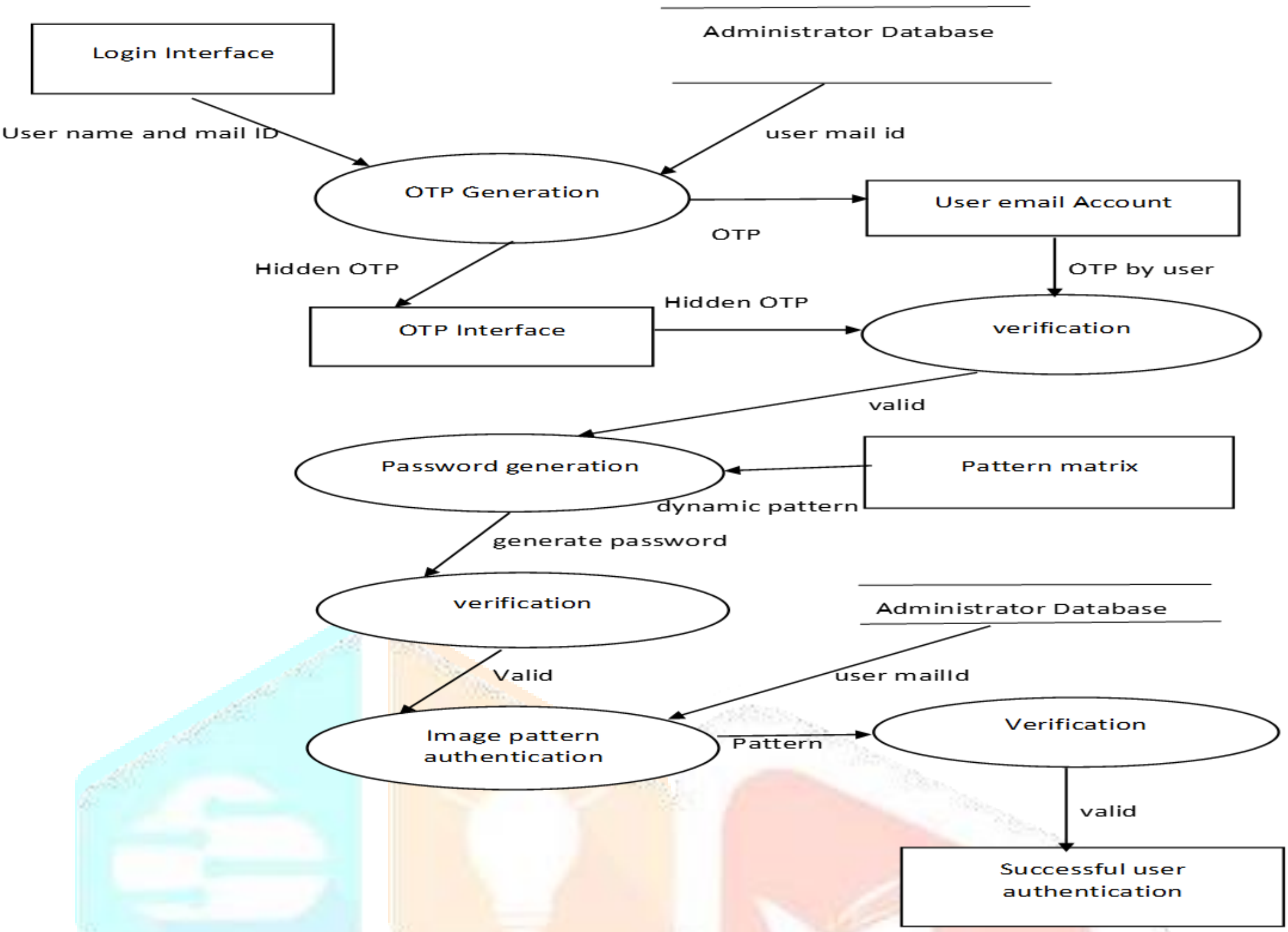


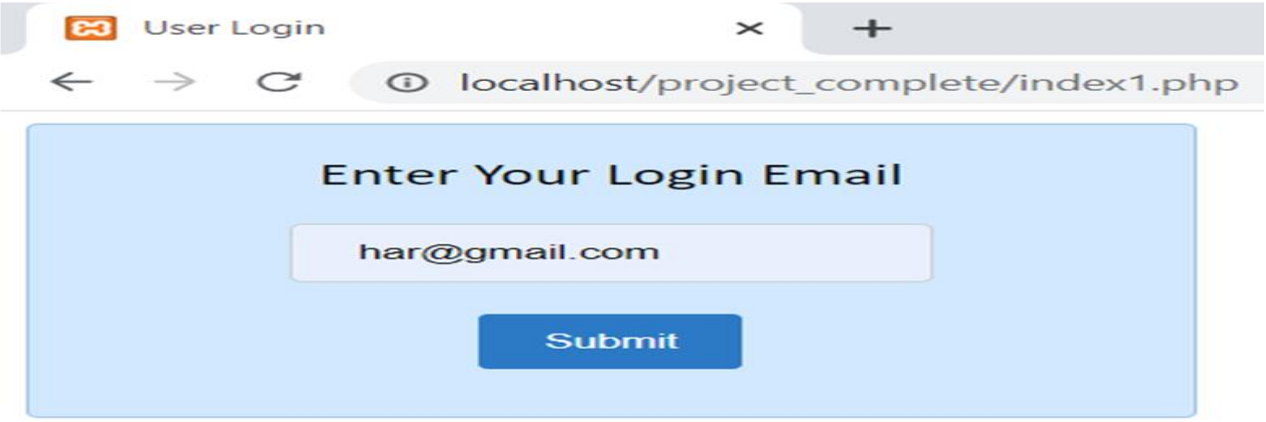
Fig 1: Flow Diagram of 3 level System

Here first the user enters the email and so using an OTP generation function the OTP is generated and stored in administer database and sent to the desired mail and finally the user gets authenticated by entering the OTP which is same as that present in database; Then after proceeding to level2 user enters the same mail along with secret string and password. The system generates a pattern matrix and based on the values user would implement a password using this all constraints and gets authenticated and proceed to next level; In the third level there will be images where the same pixels at both images need to be chosen so to get validated

VI. RESULTS

Here comes the snapshots of the 3 levels where the user is being authenticated where at level-1 using one time password and at level-2 using a virtual password means and finally at level-3 image pixel-based mapping where the same pixel points need to be chosen within the 2 images

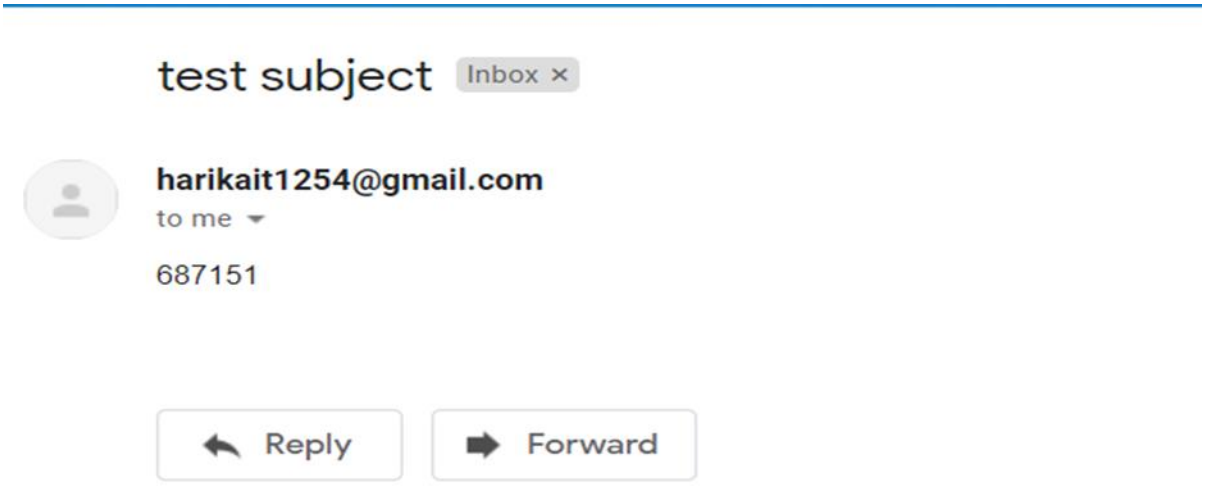
LEVEL1:



Enter Your Login Email

har@gmail.com

Fig 2: Login using Email



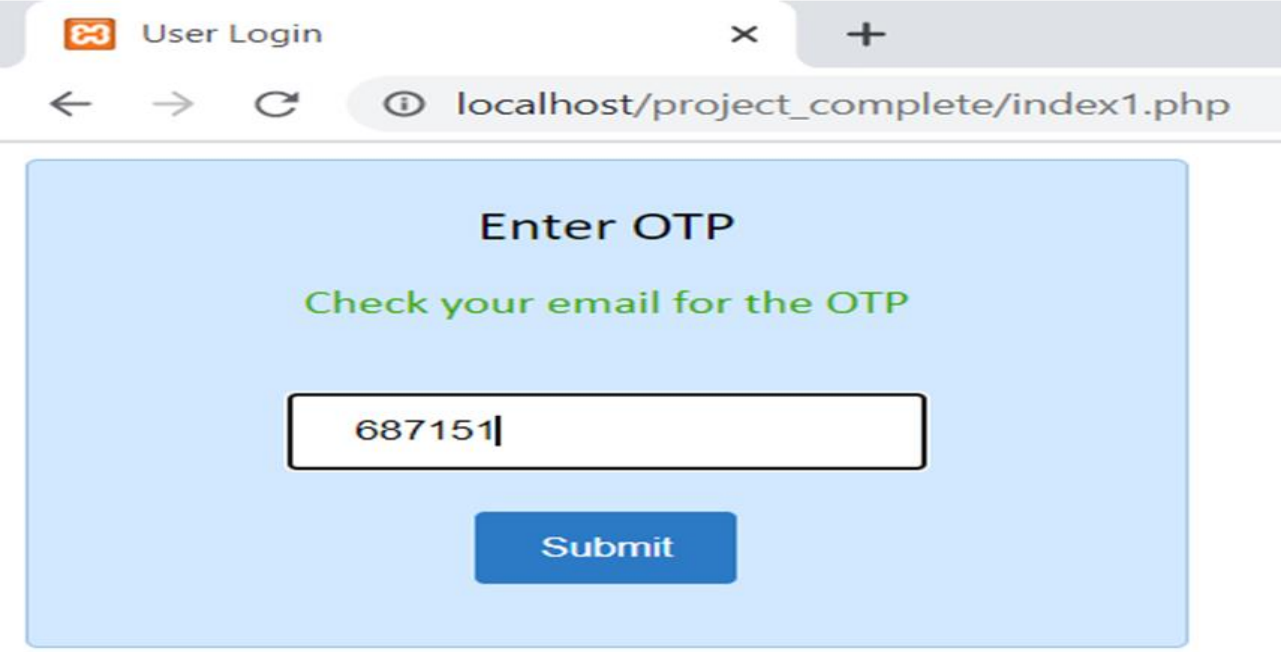
test subject

harikait1254@gmail.com

to me

687151

Fig 3: OTP sent to mail

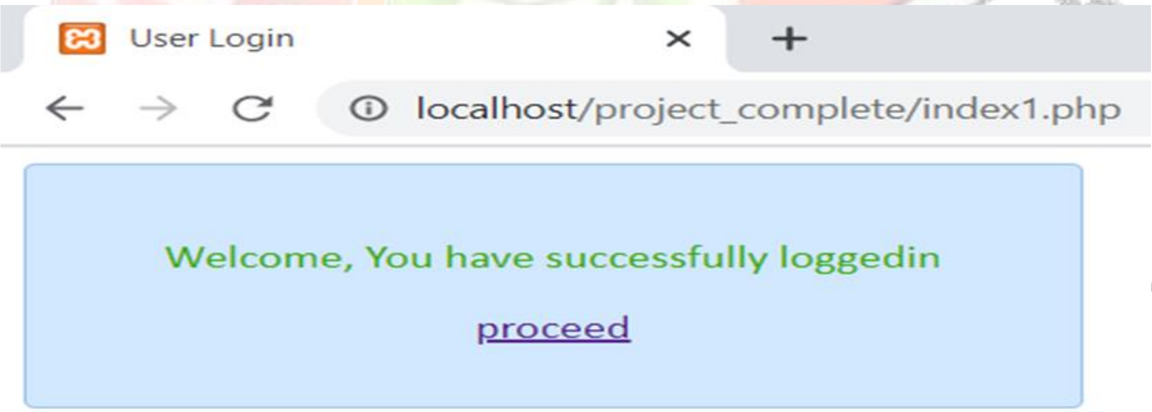


Enter OTP

Check your email for the OTP

687151

Fig 4: OTP Based Validation

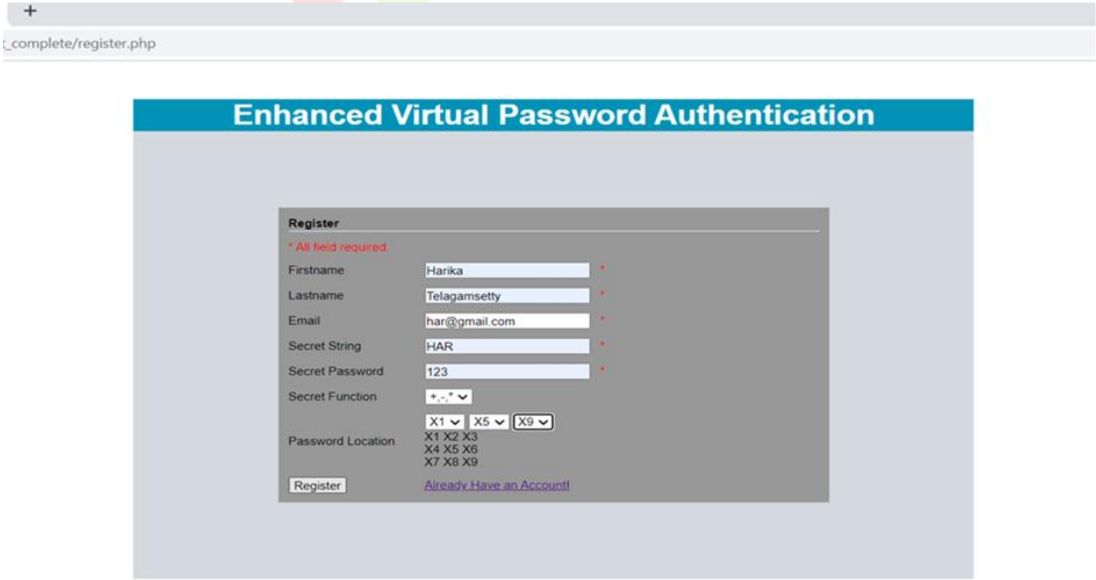


Welcome, You have successfully loggedin

proceed

Fig 5: Authenticated using OTP

LEVEL2



Enhanced Virtual Password Authentication

Register

* All field required.

Firstname Harika *

Lastname Telagamsetty *

Email har@gmail.com *

Secret String HAR *

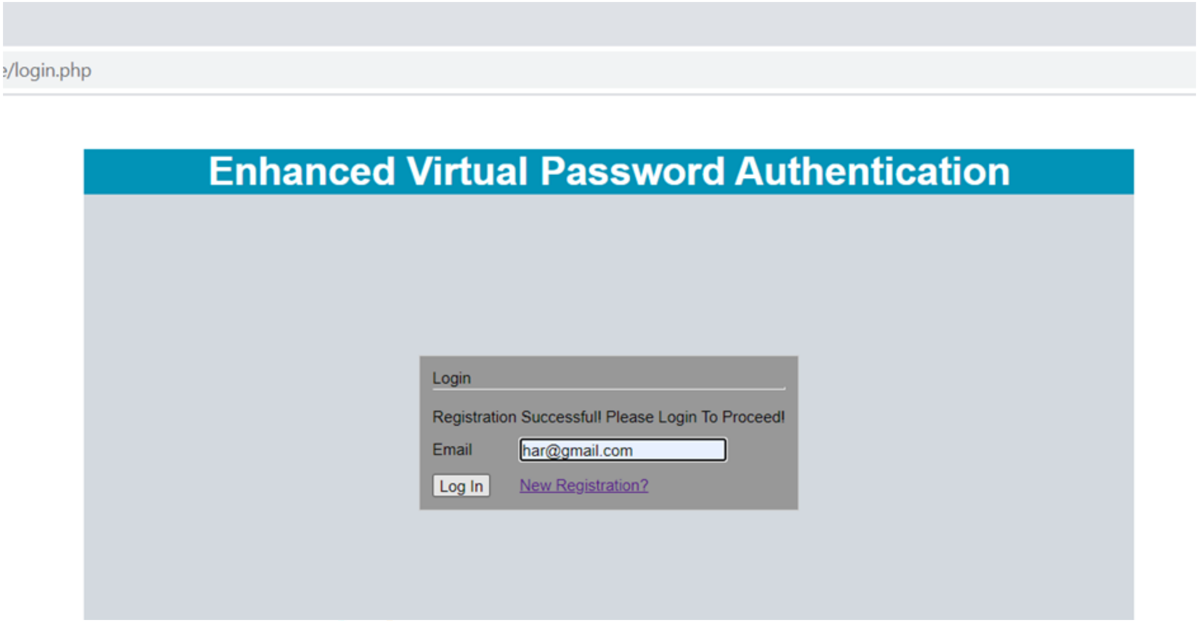
Secret Password 123 *

Secret Function +,-,*

Password Location X1 X5 X9

X1 X2 X3
X4 X5 X6
X7 X8 X9

Fig 6: Register by entering Secret String and Password


e/login.php

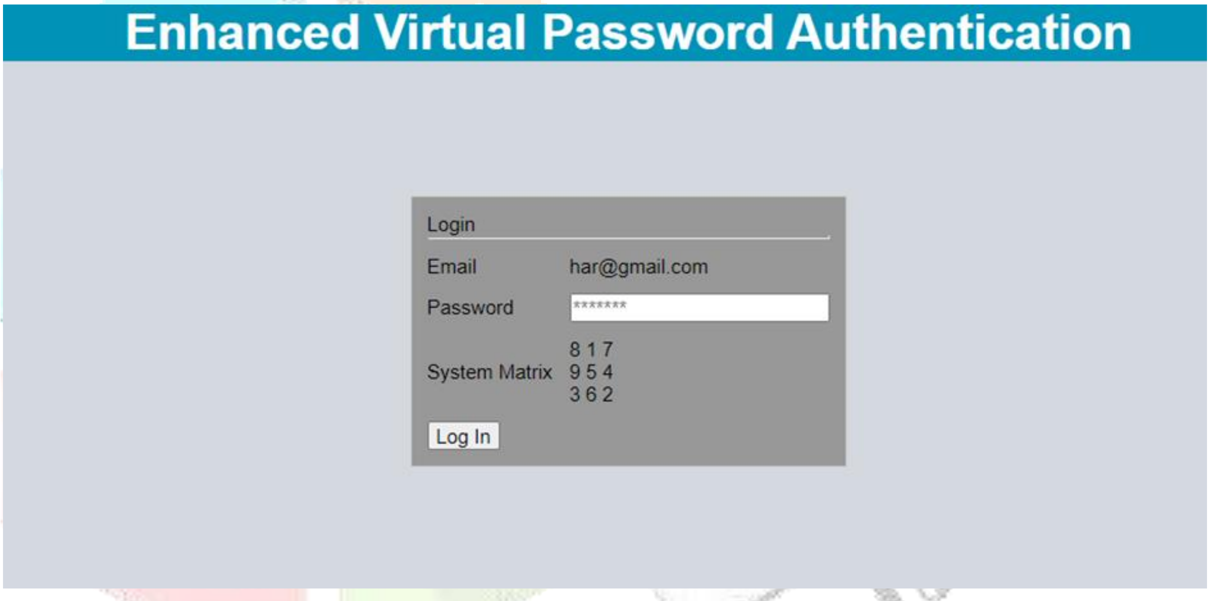
Enhanced Virtual Password Authentication

Login

Registration Successful! Please Login To Proceed!

Email har@gmail.com

Fig 7: Registration Successful


Enhanced Virtual Password Authentication

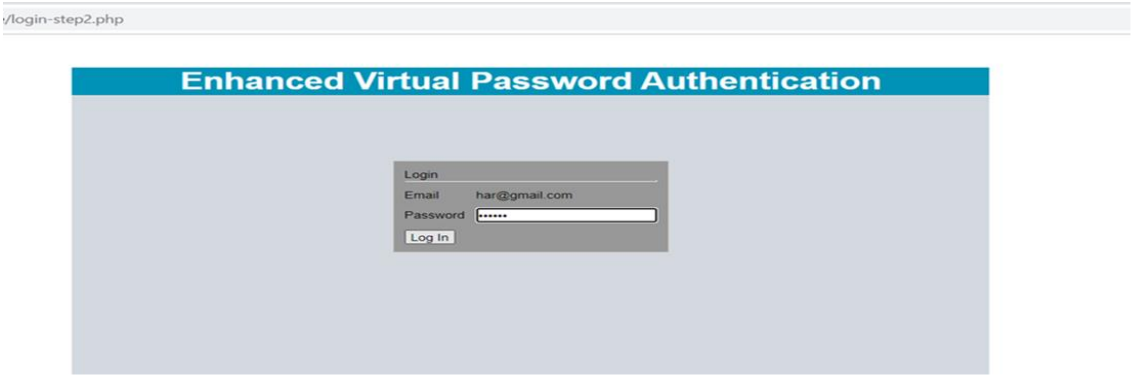
Login

Email har@gmail.com

Password *******

System Matrix
8 1 7
9 5 4
3 6 2

Fig 8: System Matrix Generated


e/login-step2.php

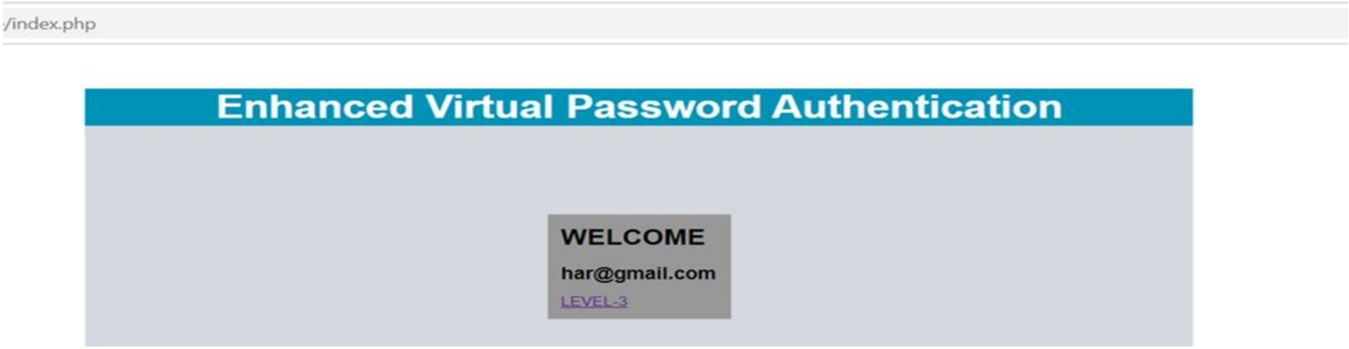
Enhanced Virtual Password Authentication

Login

Email har@gmail.com

Password ••••••

Fig 9: Password Formation (String + Password)



/index.php

Enhanced Virtual Password Authentication

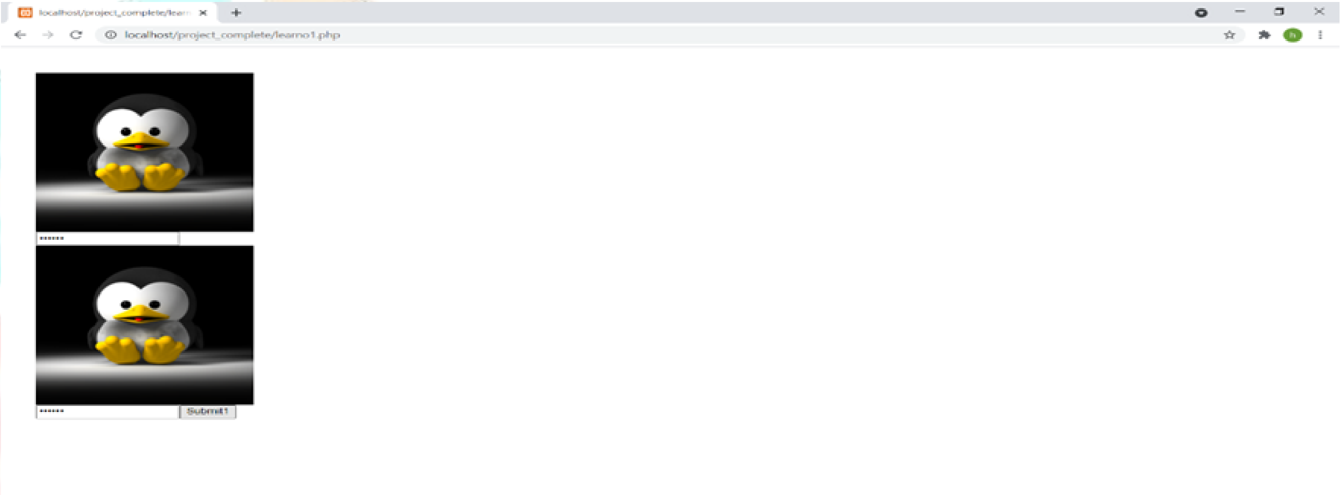
WELCOME

har@gmail.com

LEVEL-3

Fig 10: Authenticated Using Virtual Password

LEVEL3

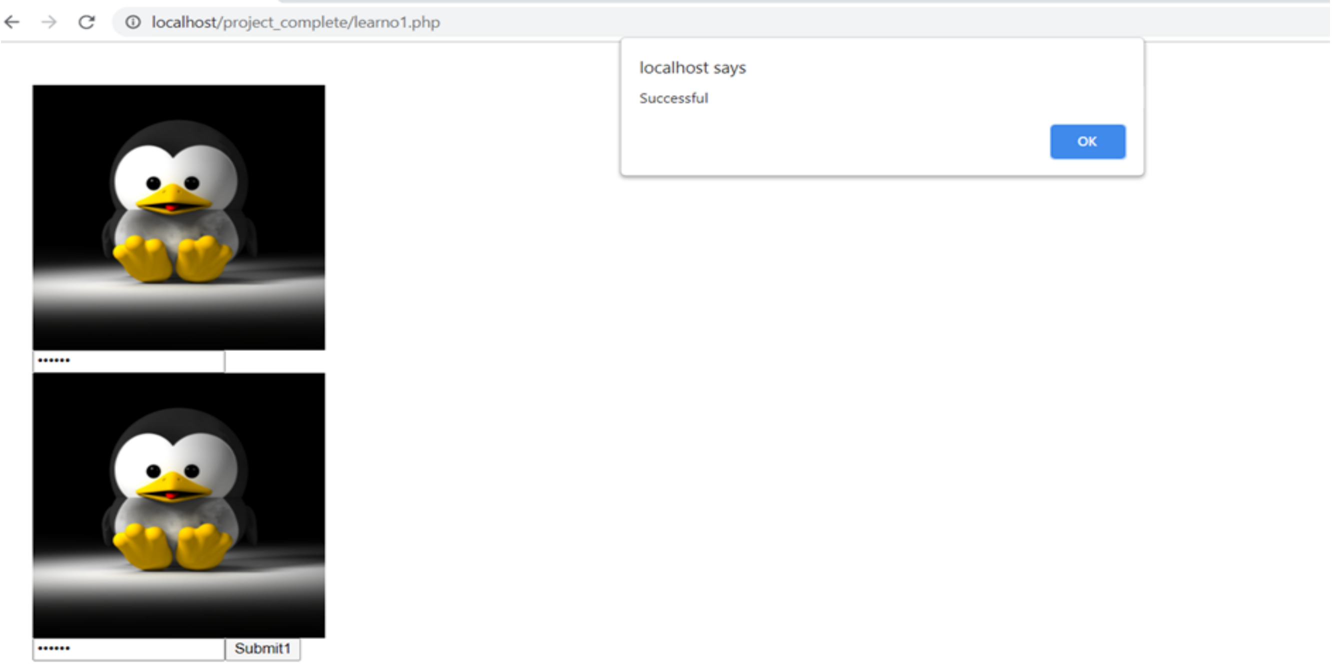


localhost/project_complete/learno1.php

••••••

•••••• Submit1

Fig 11: Image Pixel Based Authentication



localhost/project_complete/learno1.php

localhost says

Successful

OK

••••••

•••••• Submit1

Fig 12: Authenticated Using Image Pixel Method

VII. Conclusion

Importance of multi-factor authentication in overcoming the security threats and this system can be used in high security applications like Internet Banking.

The Limitation is that it may be time consuming for the user to cross multiple levels to login successfully. Keeping this limitation aside and considering the security, high level of security can be achieved through the successive levels of authentication.

VIII. Future Scope

→Users can be blocked to use the application by fixing the invalid count
→Increasing the number of levels by using some techniques (biometric, face recognition) to increase the level of security
→The user being notified when they successfully authenticate using 3 levels and start using the application

IX. References

[1] Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication, Author: Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi.

[2] S3PASA Scalable Shoulder-Surfing Resistant Textual Graphical Password Authentication Scheme, Author: Huanyu Zhao and Xiaolin Li. Richard E. Newman, Piyush Harsh and Prashant Jayaraman, “Security Analysis of and Proposal for Image Based Authentication,” 2005.

[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.

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

[5] 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.

[6] X. Suo, Y. Zhu, and G. S. Owen, ―Graphical passwords: A survey,‖ in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[7] Sagar Acharya1, Apoorva Polawar2, P.Y.Pawar. Student, Information Technology, Sinhgad Academy Of Engineering/ University of Pune. Two Factor Authentication Using Smartphone Generated One Time Password

[8] http://www.mysqltutorial.org/mysqlresources.aspx https://pdfs.semanticscholar.org/df