Student Portal with 3 Level Passwords Authentication System

B. LAKSHMI PRAVEENA[1], M. ANITHA[2], J. SUPRIYA[3] T. LAKSHMI PRIYA[4]
[1,2,3,4] *Dept. of Information Technology, VVIT, AP*

Abstract -- 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 for student portal. There are varieties of password systems available, many of which have failed due to bat attacks while few have sustained it but to a limit. In 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. Users would be given privilege to set passwords according to their wish. The project comprises of text password i.e. passphrase, colour password and pattern password for the three levels respectively.

Indexed Terms -- Authentication, textual passwords, 3-level passwords, pattern, and colour pixel.

I. INTRODUCTION

The Student Portal Authentication System with 3 level passwords is an web based application which can be used to help the members of faculty and Students in optimizing the time and effort spent in the whole process of updating and viewing the information related to their branches. This web application automates the workflow of updating and notifications to the users.

To use this web application, the members of faculty need to get themselves registered. The registered members of faculty can login into the web page for updating materials and student attendance. The Students must also be registered giving the details of their respective branch, regulation and username. After the registration is successful the student can view their respective semester attendance, related materials about their subjects.

The Admin provides the access to the faculty and students to provide the updated results and notifications.

II. MODULES

In the proposed system of 3 level passwords Authentication, the registered members of faculty and students can simply login and can access anywhere and anytime providing the required details. This also provides more security to the users account as it is a 3 level Password login. So, no one can access the others account and it is highly secured.

This web application enhances security to store the data of the users. There are mainly three modules in this application. The modules of this app are as follows:

Faculty Module Student Module Admin Module

a) Faculty Module:

The members of faculty first need to get themselves registered. Then the registered members of faculty can utilize to post the materials, attendance and the related information used for the students. They are also supposed to specify the details regarding the timetable and their lecture hours

b) Student Module:

The Student makes use of this after the completion of registration to access the materials and to view the results and notifications generated by the faculty and admin of his/her department.

III. 3-LEVEL PASSWORD SCHEME

In this paper, we propose a multifactor authentication scheme that combines the benefits of the existing authentication schemes and thereby, overcomes the pitfalls of the currently used authentication schemes

[1]. Below are some of the requirements we attempted to satisfy:

1. The new scheme stated should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall-based technique, recognition-based technique, textual password, color pixel selection and pattern password.

2. Users ought to have the freedom to select the first two levels of password i.e. the selection of textual and color pixels in the same order in the first and second levels of password respectively. This freedom of selection is necessary as the users are different and each user may have different requirements. Hence, the user's freedom of selection is important to ensure high user acceptability.

3. The new scheme should provide easy to remember secret keys that are very difficult for intruders to guess.

4. The new scheme should provide secret keys that are difficult to share with others and which are not easy to write down on paper.

5. The new scheme should provide secret keys that can be easily changed or revoked.

Based on the aforementioned requirements, we propose our contribution, i.e., the 3-Level password authentication scheme. The three main levels of the authentication system are described below.

a) Textual Password:

The first level i.e., the textual password simply means the selection of alphabets, characters and numbers. The images provided are commonly used, user friendly and easy to remember images. For example, we can select numbers, characters and alphabets. During registration process user need to set a password for the account.

b) Color Pixels:

After textual password, we move to the second level i.e., the selection of color pixels. The user can select a single color pixel from the different blocks of colors provided. For example, we can set a count, say one. So the maximum limit of color pixel selection will be set to one. During authentication phase, the previously textual password should be chosen in the first level and then the user will be redirected to the second level i.e. the color pixel selection, where the user selects the same color pixel chosen in the registration phase. In case of any invalid selection of textual or color pixel the system will be locked automatically after few trials based on the count given.

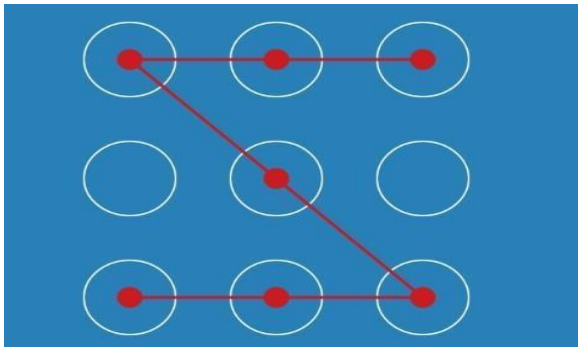
c) Pattern Password

Pattern locks, however, are quite different. Although they look quite confusing and complex, they're actually not. In order to explain why not, we'll need to look at the maximum number of permutations. When you first start with your pattern, you have nine points to choose from. This will be our *first* factor. Let's take the choice which gives us the most amount of options: the middle point. From here, you can pick any of the eight others as your second point. This will be our *second* factor. Whatever point you picked will give you the number of available neighbouring points. A corner point leaves only two options, while a side point gives you four — the two corners and the adjacent side points.

But let's ignore the fact that you may (or may not) have to pick a neighbouring point. If you can go to whichever point you'd like next, you'll only have seven available options left as you can't pick a point twice the reason why each factor's value is declining. This is our *third* factor.

The *fourth* and *fifth* factors would, ideally, be six and five. Therefore, under ideal conditions, the maximum amount of permutations you can get with a 5-point pattern is 9*8*7*6*5=15,120. Even if you went ahead and used a 6-point pattern, you'd only get a total of 60,480 permutations. Compared to what passwords offer, that's absolutely nothing.

Admittedly, no one with a reasonable mind will want to manually try out 15,120 different possibilities, but the ratio of permutations of a 5-character password compared to a 5-point pattern is almost 390,536:



IV. CONCLUSION

The Student portal Authentication system with three level passwords is developed to facilitate, student, administrator easy processing for students in educational institutions. Manually, this consumes a lot of time, effort and paper work. And also if the concerned authority is not available, the task of logging in becomes complicated .So, this web application overcomes all these limitations and offers a great deal of help at each and every stage in the whole process of communicating to students.

V. FUTURE SCOPE

This project Student portal Authentication system with three level passwords has been developed in such a manner, that the future requirements of the user are met. The project is flexible to adapt the changes efficiently without affecting the present system. In future, there can be a provision to update attendance, results, and notifications through the web application.

We are also planning to implement the web application on various other platforms like Windows and ios. This is the future scope of our project.

REFERENCES

- Web Resources:

[1] http://www.tutorialspoint.com/mysql/
[2] http://www.mysqltutorial.org/mysql-resources.aspx
[3] https://pdfs.semanticscholar.org/df89/7ed3b8f02231aea5887b293e3c5b599ed379.pdf
[4] https://www.thieme-connect.com/products/ejournals/abstract/10.1055/s-0038-1634610
[5] https://www.tutorialspoint.com/java/index.htm
[6] https://www.ijarse.com/images/fullpdf

- Book Resources:

[1] MySQL CookBook,Paul
[2] MySQL development by Luke Welling.
[3] Java Complete Reference, HERBERT SCHILDT
[4] EFFECTIVE JAVA (2nd) Edition, JOSHUA BLOCH.
[5] HTML and CSS, JON DUCKETT