GOVERNMENT POLYTECHNIC, NANDED

MICRO PROJECT

Academic year: 2020-21

TITLE OF THE PROJECT

Three Level Password Authentication System

Program: Information Tech. **Program code:** IF 6I

Course: NIS **Course code:** 22620

Name of Guide:- S. N. DHOLE

MAHARASHTRA STATE

BOARD OF TECHNICAL EDUCATION

Certificate

This is to certify that Mr. **Vaibhav Dawane, Shivhar Bane, Harsh Zanwar**

Roll No. 1568, 1547, 1570 of **6th** Semester of Diploma in **Information Technology**

of Institute, GOVERNMENT POLYTECHNIC has completed the **Micro Project**

satisfactorily in Subject - **NIS (22620)** for the academic year 2020 - 2021

as prescribed in the curriculum.

Place: Nanded

Date: Exam. Seat No: .....

Subject Teacher	**Head of the Department**	**Principal**
S. N. Dhole	S. N. Dhole	DR. G.V. GARJE

WEEKLY PROGRESS REPORT

TITLE OF THE MICRO PROJECT:- Three Level Password Authentication System

WEEK	ACTIVITY PERFORMED	SIGNOFGUIDE	DATE
1ST	Discussion and finalization of Topic		
2ND	Discussion and finalization of Topic		
3RD	Preparation and submission of Abstract		
4TH	Literature Review		
5TH	Collection of Data		
6TH	Collection of Data		
7TH	Collection of Data		
8TH	Collection of Data		
9TH	Discussion and Outline of Content		
10TH	Formulation of Content		
11TH	Editing and 1st Proof Reading of Content		
12TH	Editing and 2nd Proof Reading of Content		
13TH	Compilation of Report and Presentation		
14TH	Seminar		
15TH	Viva-voce		
16TH	Final submission of Micro project		

Sign of the student **Sign of the faculty**

S. N. Dhole

ANEEXURE II

Evaluation Sheet for the Micro Project

Academic Year: 2020-21 **Name of the Faculty:** S. N. Dhole

Course: NIS **Course code: 22620** **Semester: VI**

Title of the project: Three Level Password Authentication System

Cos addressed by Micro Project:
A : Apply User Authentication Methods.
B : Apply Measures To Prevent Attacks

Major learning outcomes achieved by students by doing the project

(a) Practical outcome:
1) Deliver report effectively.

(b) Unit outcomes in Cognitive domain:
1) Prepare the points for computer presentation.
2) Make seminar presentation.

(c) Outcomes in Affective domain:
1) Function as team member.
2) Follow Ethics.
3) Make proper use of computer and Internet

Comments/suggestions about team work /leadership/inter-personal communication (if any)

……

……

Roll No.	Student Name	Marks out of 4 for performance in group activity (D 5 Col. 8)	Marks out of 2for performance in oral/ presentation (D 5 Co 1.9)	Total out of 06
1547	Shivhar Bane			
1568	Vaibhav Dawane			
1570	Harsh Zanwar			

(Signature of Faculty)

S. N. Dhole

INDEX

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. 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.

Levels in the system

First Level:

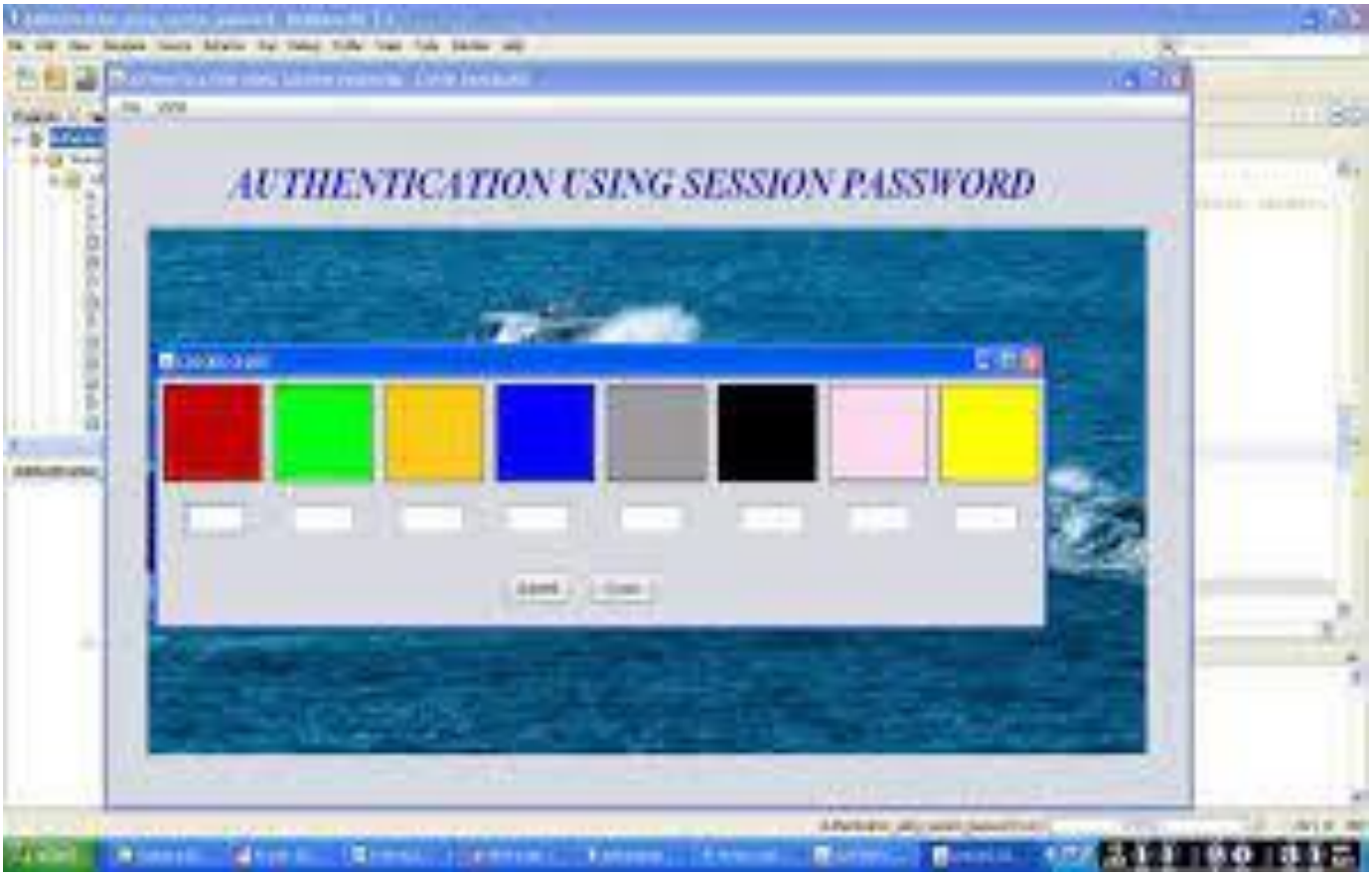
The first level is a conventional password system i.e. text based password or a passphrase. Users would have to set a text password initially based on some specifications.

1.

2.

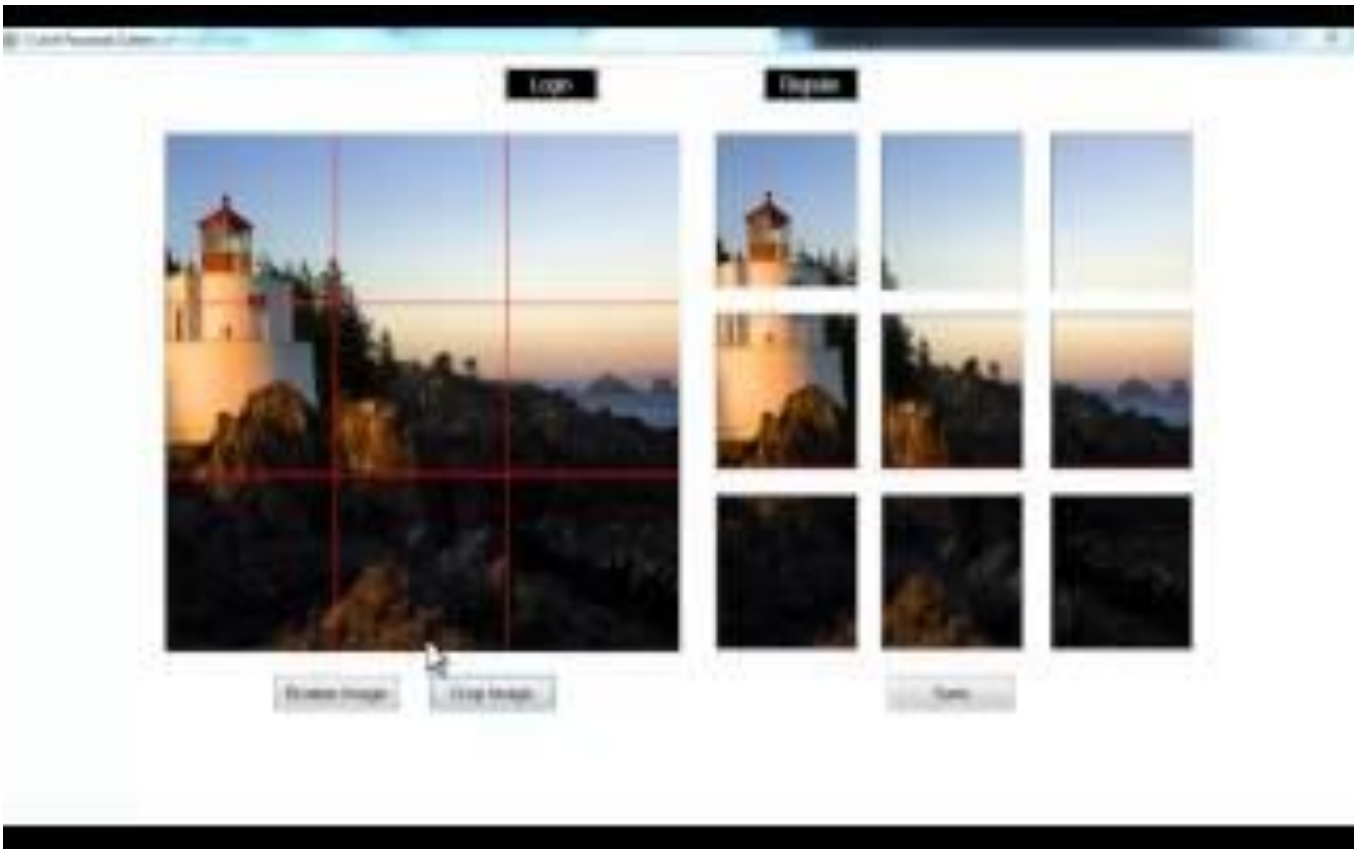
Second Level:

The second level is an image based password where users can upload their desired image into the system and then create password by segmenting it and assigning them serial numbers. During login process the system will automatically disperse the image segmentations and users have to arrange it as set by them initially.



Third Level:

The third level is a graphical password method where users have to set password based on some color combinations through RGB button combinations.



Advantages

- The system is user-friendly and has simple interface.
- Provides strong security against bot attacks or hackers.
- Users can set or upload their own images.
- Protects systems vulnerable to attacks.

Disadvantages

- The only disadvantage is if users forget the password, it cannot retrieve it.

Features:

- Users would be given a registration form that has to be filled with required details.
- Next users would be asked to set password for first level, second level and third level subsequently.
- After the passwords are set for the three level users can now login into the system.
- While login the system will ask for the first level password. On entering correct password, second level password is asked and then third one.
- After the user has provided correct password in the third level, he gets authenticated and can now access the system.

Conclusion

The three level security approach applied for a framework makes it exceptionally secure alongside being more easy to understand. 3-Level Security framework is certainly is a tedious methodology, as the client needs to navigate through the three degrees of security, and should allude to his email-id for the one-time computerized created secret word. In this way, this framework can't be a reasonable answer for general security purposes, where time intricacy will be an issue.

Sources Used

1. **https://www.google.com/**
2. **https://en.wikipedia.org/wiki/Main_Page**