

**Project Report**  
**On**  
**Color Matrix Based Virtual Password System**

*Submitted to*  
**Government College of Engineering, Nagpur**  
*in partial fulfilment of the requirement for the degree of*  
**BACHELOR OF ENGINEERING**  
*in*  
**Computer Science & Engineering**

**Submitted By**

**Anik Mukherjee**  
**Himanshi Darvekar**  
**Akash Zalke**  
**Adwait Padhye**

**under the Guidance of**

***Dr. Latesh Bhagat***



**Department of Computer Science & Engineering**  
**Government College of Engineering**  
**New Khapri, Nagpur-441108(M.S)**  
**2020-2021**

## **CERTIFICATE OF APPROVAL**

Certified that the project report entitled Color Matrix Based Virtual Password System has been successfully completed by \_\_\_\_\_ under the guidance of Dr. Latesh Bhagat and it is submitted to Department of Computer Science & Engineering.

Signature

Dr. Latesh Bhagat  
H.O.D,CSE

Signature

Dr. Latesh Bhagat  
Project Guide



**Department of Computer Science &Engineering**  
**Government College of Engineering**  
**New Khapri, Nagpur-441108(M.S)**  
**2020-2021**

CONTENTS	PAGE NO.
Title Page	i
Certificate of Approval	ii
Table of Contents	iii
Abstract	...
Chapter 1: Introduction	1
1.1 Overview	1
1.2 Problem and Motivation	1
1.3 Purpose and Objective	2
1.3.1 Purpose	2
1.3.2 Objective	3
Chapter 2: Literature Survey	5
2.1 Overview	5
2.2 Existing Systems	6
2.2.1 Drawbacks of Existing Systems	7
2.3 Need for Proposal	8
Chapter 3: Work Done	9
3.1 Stipulated Development	9
3.2 Hardware Setup for Development	9
3.3 Software Setup for Development	10
3.4 Procedure adopted for development of the User Interface	10
3.5 Software development life cycle model adopted:	11
3.6 Progress snapshots of the project:	12
Chapter 4: Summary and Conclusion	19
4.1 Summary	19
4.2 Conclusion	19
Chapter 5: Literature Cited	20

## **ABSTRACT**

Shoulder surfing attacks have proven to be a great bane for information and technology systems since their very inception. While great strides have been taken to improve the security of systems internally against hacks and viruses, the same progress has not been made to circumvent the very basic intrusion made by human eyes.

While there are no reliable statistics on the prevalence of shoulder surfing attacks, a 2016 study conducted by Memon and Nguyen found that 73 percent of mobile device users surveyed reported that they had observed someone else's PIN (although not necessarily with malicious intent), and a 2017 study of shoulder surfing awareness presented at the ACM Conference on Human Factors in Computing Systems reported that 97 percent of those surveyed claimed awareness of a shoulder surfing incident in everyday life, and that in the majority of cases, victims were unaware that they were being observed.

Password authentication systems form the basis of most of the contemporary businesses, medical, financial, entertainment, and technological industries. A simple glance from an onlooker can give away the login details of an individual or an organization. Incidents such as this can prove extremely costly, but at the same time, are extremely difficult to avoid. As a result, having such an underwhelming solution to an extremely serious security risk is far from ideal.

In this project, we look to address this issue of shoulder surfing attacks by coming up with a novel password security system which builds on the currently used system to great effect.

# 1. INTRODUCTION

## **1.1 Overview:**

Color Matrix Based Virtual Password System uses a color matrix which is randomly generated on each login attempt. This color matrix maps a single color to multiple characters which are supported in a password. This basic functionality of this app allows an added layer of protection by introducing an additional layer of abstraction between the user and the onlooker.

When an individual is trying to enter their password using this virtual password system, instead of entering their actual password, they would enter the color associated with the corresponding characters by the color matrix. The actual password would not be exposed to any observers, as a result, and only the corresponding colors would be. However, as each color is mapped to multiple characters, the password would be protected.

As the color matrix is randomized at each login attempt, even after multiple attempts of password theft, any malicious individuals would be unable to correctly identify the password.

## **1.2 Problem and Motivation:**

In today's high technology environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing.

Today's information system the security is largely supported by password for authentication process. The most of password contains alphanumeric and special characters it is highly vulnerable. To overcome the drawbacks of traditional method

we propose new authentication method to abolish well known Security threats like brute force and shoulder surfing attacks.

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder. Unauthorized users watch the keystrokes inputted on a device either at close range (by directly looking over the victim's shoulder) or from a longer range with, for example a pair of binoculars or similar hardware. The advent of modern-day technologies like hidden cameras and secret microphones makes shoulder surfing easier and gives the attacker more scope to perform long range shoulder surfing. A hidden camera allows the attacker to capture whole login process and other confidential data of the victim, which ultimately could lead to financial loss or identity theft.

Irrespective of how cautious a person is when entering their password, or how quickly they try to do it, it is almost impossible to avoid being shoulder surfed if the intruder so desires. The presence of hidden cameras can not be identified, so there is no safe place to hide your screen while entering the password. Besides this, cameras used for shoulder surfing also have advanced capabilities such as zooming in to the device screen, slowing down the captured video, and identifying key strokes inputted by a person.

In an attempt to overcome this issue, and reduce the paranoia around entering passwords in public, the Color Matrix based Virtual Password System finds a novel way around this problem by completely eliminating the risk of giving away your password to an unwanted observer.

### **1.3 Purpose and Objective:**

#### **1.3.1 Purpose:**

The main purpose of the Color Matrix based Virtual Password system is to generate a Color Matrix which maps a color to multiple characters of a password or PIN and randomly generate this matrix on each login attempt. The application also comes with a simple, elegant, and extremely intuitive User Interface which makes it possible to have a hassle-free experience on each login attempt made by the user.

This application also helps abolish the paranoia around entering your password in a public space, and is also a huge step forward with regards to public safety and privacy concerns which have increased due to the normalization of public monitoring systems in cities.

#### **1.3.2 Objective:**

- Providing a novel password protection system
- Minimize shoulder surfing attacks
- Decrease paranoia around entering passwords
- Help decrease the concerns about social monitoring systems
- Help protect the integrity of an individuals financial and social accounts
- Maintain the integrity of an organizations crucial business, commercial, and strategic information
- Providing a simple and intuitive User Experience while entering a password
- Achieve great leaps in mitigating public privacy concerns
- Make the installation of cameras to capture passwords redundant
- Help in achieving greater public security

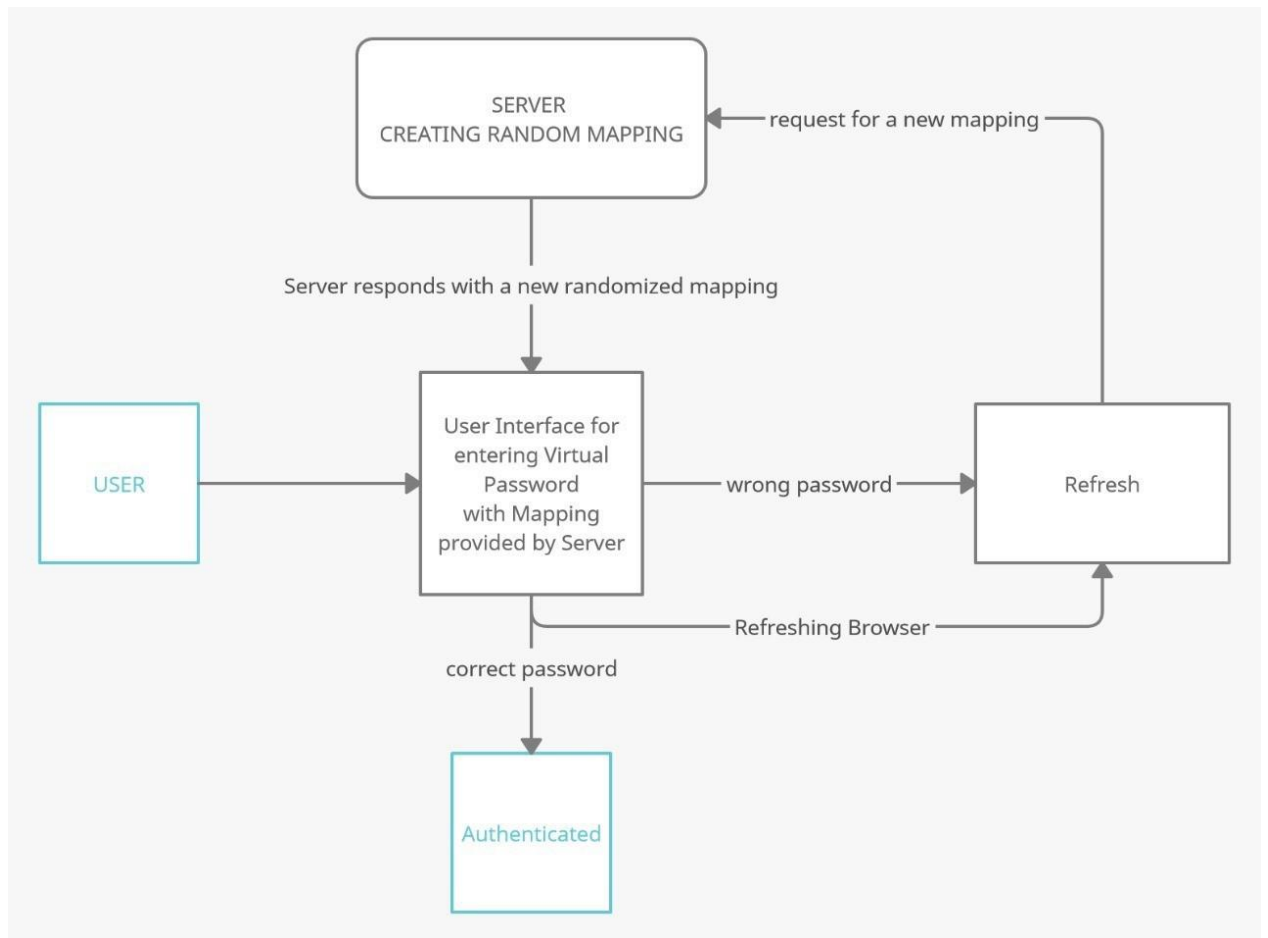


Fig. 1.1 Data Flow Diagram

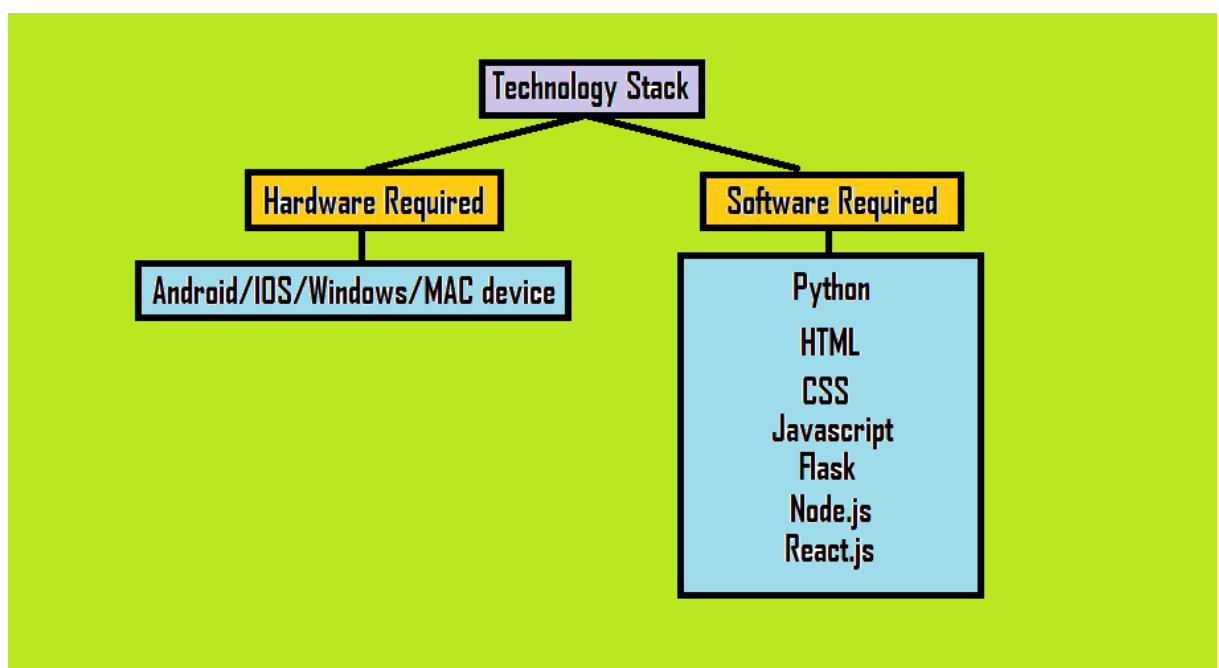


Fig. 1.2 Technology Stack



## **2. LITERATURE REVIEW**

### **2.1 Overview:**

The practice of shoulder surfing is a criminal act, where thieves steal your personal data by spying over your shoulder as you use a laptop, ATM, public kiosk or other electronic device in public. The practice long predates smartphones and laptops, and goes back to when criminals spied on pay phone users as they punched in their phone card numbers to make calls. From there, thieves moved to observing their victims key in PINs while using ATMs, paying for gas at self-service pumps or even making a purchase in a store.

Shoulder surfing can occur anytime you're sharing personal information in a public place. That includes not only ATMs, payment kiosks and PIN pads, but just about any place where you use a laptop, tablet or smartphone to input personal data. This poses a great danger to public security, as no public space is safe for accessing personal data on your electronic devices. This problem is further cemented with the transition towards e-commerce and online banking and UPI transactions being front and center of the next big technological convenience provided by mobile devices. Losing the password of your UPI app, or e-commerce app to a perpetrator can lead to huge financial losses. Despite this risk, the applications are seldom held liable to such damages as these incidents come under a legal gray area where neither the platform holders, application developers, nor the user himself can be blamed completely.

This problem can also be observed on an industrial scale, where an employee may expose the password of an account of their company or organization to a competitors spy or a camera installed by them. This can prove disastrous for the company as a lot of important information such as financial reports, trade secrets, patents, employee records, customer records, business transactions, etc. will now be available with their competitors. Not only this, the data corresponding to their costumers may also be leaked by the hackers which would put a large number of people in danger. Also, the organization who have been hacked would have to take responsibility as the could not

protect the public data effectively. As this can happen to any of the employees in the organization, and lead to a slippery slope of damages forced upon a lot of individuals, this leads to a very delicate situation where protecting the accounts of the company and the individuals are of paramount importance.

Another reason it is more important than ever to pay attention to this problem is because the inventions in camera technologies and computer vision algorithms have made it easier than ever for shoulder surfing attacks. Key stroke detecting algorithms can predict your password by looking at your hand movements and gestures, even when your screen or keyboard is partially occluded from the cameras view. Surveillance cameras are also commonplace in most buildings and complexes these days, and as a result, it is easier than ever to hide spying cameras for capturing passwords.

Many solutions have been adopted and invented over the years in an attempt to overcome this problem. However, it is readily evident that a sufficiently effective solution is not yet available which would completely solve this issue. A virtual password can be used to find a way around this issue by only ever exposing the virtual password in a public space. Using a randomized color matrix adds another layer of randomness to the equation as it is impossible to predict how the mapping is going to work next on the back-end. This provides an extremely effective and elegant solution to what has proven to be a rather difficult problem to solve.

## **2.2 Existing Systems:**

### **A. Pattern based unlocking system:**

This type of locking system utilizes a pattern for protecting access to particular areas instead of a character based password or number based PIN code. This type of locking system is mainly observed in smartphone devices to prevent unauthorized access into the phone.

### **B. One-Time Password Protection:**

A One-Time Password protection is used to provide a single use password, which usually consists of a group of digits. This password is sent to the user either via

SMS on their phones, or on the e-mail address that they have provided. This provides an additional layer of protection by way of Two Factor Authentication (2FA).

### **C. Face Detection:**

Face detection systems have recently emerged as being useful in locking mechanisms, by only allowing access to a certain user by simply scanning their face with a camera and using Computer Vision techniques to match the scanned face with stored data. This provides ease of access to the authorized user, while keeping unauthorized users out. This system is mainly implemented in smartphones and door locking mechanisms.

### **D. Fingerprint locks:**

Fingerprint sensor-based locks are often found in most modern smartphones and laptops, and are proving to be a useful alternative to traditional password based locking systems. They scan the fingerprint of the user, and only provide access if it matches with the recorded fingerprint. This technique is not only used to lock phones and laptops, but is now frequently being used to lock particular applications such as social media apps as well as UPI applications.

## **2.2.1 Drawbacks of existing systems:**

### **A. Pattern based unlocking system:**

- While patterns are quite a lot more difficult to shoulder surf than traditional passwords by eye, they can still be easily copied with the use of a camera.
- It can often be quite difficult for individuals to remember complex patterns.
- Older people or those with special needs often find it difficult to draw intricate patterns.

### **B. One-Time Password Protection:**

- This is not really a replacement for traditional password systems, but a supplement to it. This system can also be used in conjunction with our Matrix based system for greater security.
- It causes difficulties in logging in if a user does not have his mobile phone on hand.

**C. Face Detection:**

- Not very secure, as a person may have his face scanned by another individual without being aware of it.
- Not very reliable as sometimes it may unlock devices or applications unintentionally.
- Only work if a device has a camera.

**D. Fingerprint locks:**

- Only work if a device has a fingerprint sensor.
- Not very secure, as a person may have his finger scanned by another individual without being aware of it.
- Fingerprints of an individual can change overtime, and may also get damaged in an accident.

**2.3 Need for proposed system:**

With the growing reliance of organizations and individuals on technology for their financial and personal needs, the opportunity for exploitation for the same has sky rocketed. This has also incentivized perpetrators and criminals to find new and more efficient ways to steal peoples information.

However, the most simple way of stealing ones data still remains one of the simplest. Shoulder surfing attacks have plagued password based security systems which work on the basis of encryption on the back-end since their very inception. Although steps have been taken to raise awareness to help avoid shoulder surfing attacks, they remain largely prevalent in a substantial capacity.

Many new systems have been created to try to replace the password based system, however they each have their own flaws. Be it reliability, scalability, ease of use or any of the other myriad of deficiencies prevalent in the system, none of the emerging technologies have managed to completely and reliably replace password authentication.

The color matrix based virtual password system builds on the existing password encryption system to provide a user friendly, safe, robust, and reliable solution to the password protection problem, without any of the aforementioned drawbacks.

### **3. WORK DONE**

#### **3.1 Stipulated Development:**

As per the synopsis of the Color Matrix Based Virtual Password System project, the project development team has completed 100% of the total project work that is needed to deem the project as complete by the faculty and the project development team. All of the work in the project was divided in three phases and the work done described below stands true for the first phase of the project that involves the development of the backend, second phase involves development of the user interface and the third phase involves hosting.

#### **3.2 Hardware Setup for Development:**

The development of the user interface for this project involved a website. It was undertaken on three different systems using three different systems working on three different operating system Linux, MacOS and Windows.

The website was developed using python, flask as a backed framework running on Windows 10 home operating system having Intel i3 dual core processor and 4GB random access memory and 1TB of hard drive as secondary storage.

The hardware that was used was working as per the requirements of the team.

#### **3.3 Software Setup for Development:**

The development of the user interface of this project for the web application was undertaken using Flask framework developed using HTML, CSS and Jinja2 templating programming language. The coding for the application was done on Microsoft Visual Studio Code also called VSCode, configured with python plugin

Additionally, a Local Host server was put up to test the application without running it on an actual Internet which worked as a testing environment

The development of the user interface of the website was undertaken using flask framework and JavaScript programming language. Visual elements of the website were

developed using Hypertext Markup Language (HTML), Cascading Style Sheets (CSS) and Bootstrap framework

Microsoft Visual Studio Code also called VSCode was used for the writing and editing the code for the website. Mozilla Firefox was the web browser of choice for testing the website

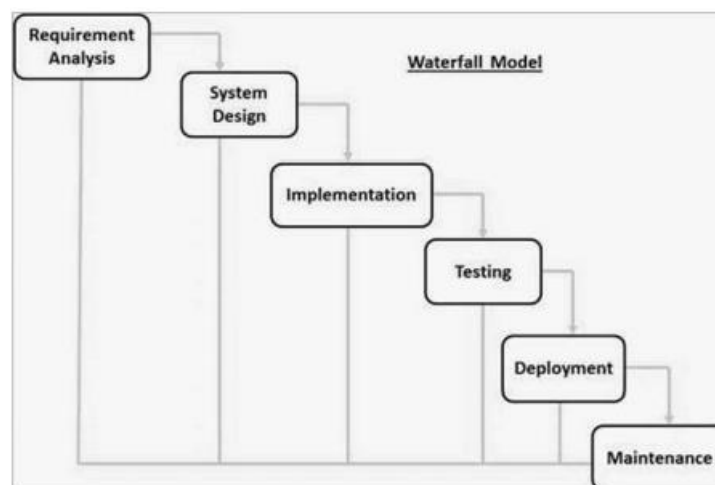
### **3.4 Procedure adopted for development of the User Interface:**

A robust procedure was developed for the development of the user interface of the applications and the website. Feedback formed the backbone of this procedure so as to make sure an ideal, foolproof and user friendly, user interface is developed across the board for all platforms. 11 The procedure is described in detail below.

1. Wireframes are developed on a page.
2. The wireframes are roughly laid out on the device.
3. Feedback is taken from the team regarding the useability and design.
4. Step 1 to Step 3 are repeated again until no further improvements are suggested by the team

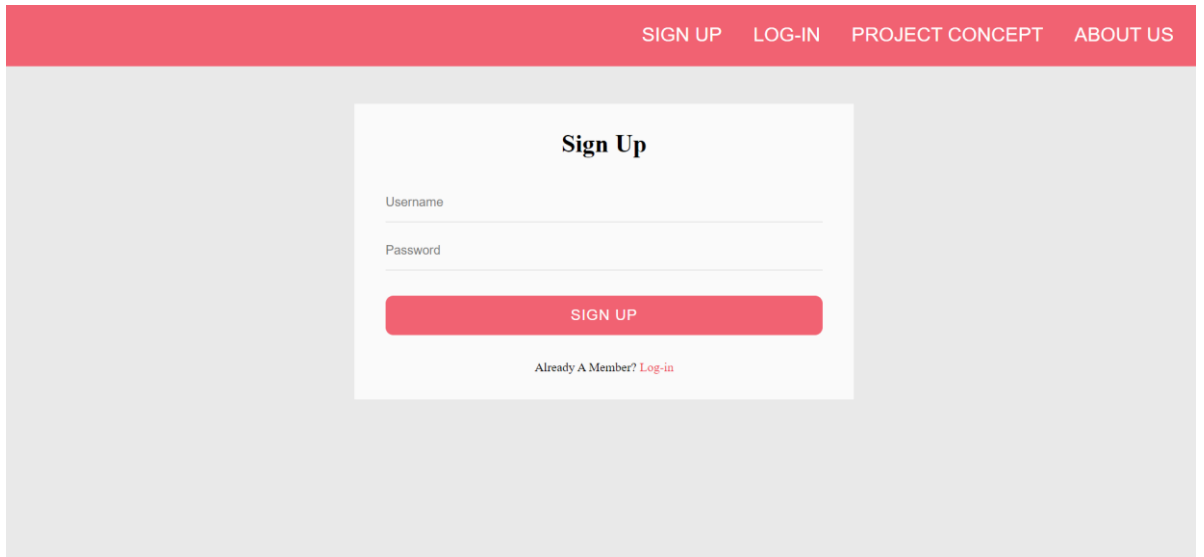
### **3.5 Software development life cycle model adopted:**

Proper selection of a software development life cycle allows the team to develop the system efficiently. Furthermore, it allows the team to deliver most of the features and to deliver the project on time. The SDLC model that the team selected is the Waterfall SDLC model. The selection was done on the basis of the two points listed above



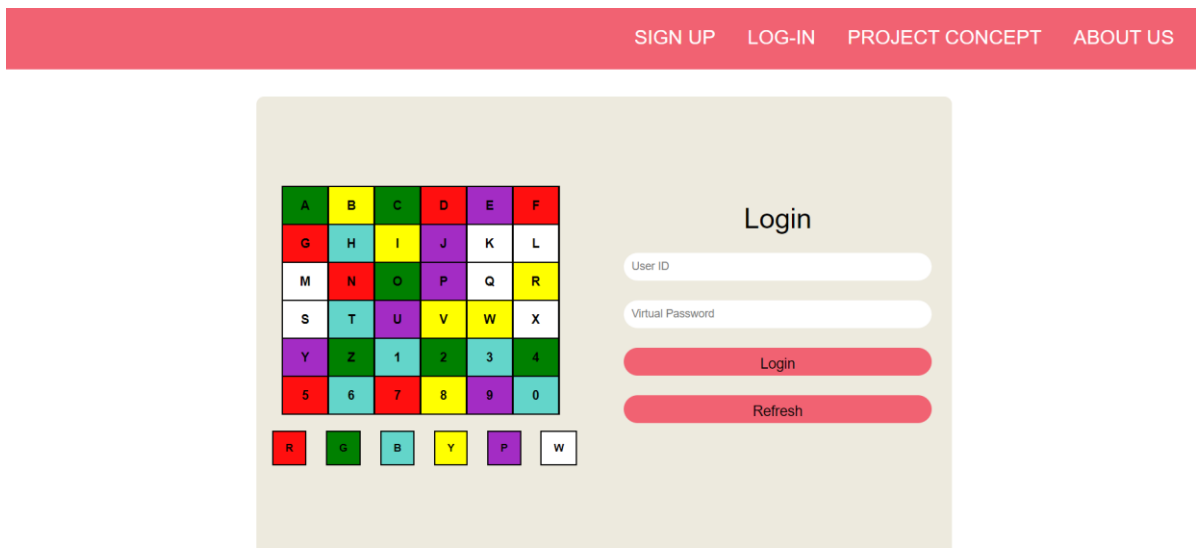
### 3.6 Progress snapshots of the project:

Below are snapshots of the User Interface developed :



A screenshot of a web application's 'Sign Up' page. The page has a red header bar with navigation links: 'SIGN UP', 'LOG-IN', 'PROJECT CONCEPT', and 'ABOUT US'. The main content area is light gray. In the center, there is a white card with the title 'Sign Up'. Below the title are two input fields: 'Username' and 'Password'. A red button labeled 'SIGN UP' is positioned below the password field. At the bottom of the card, there is a link that says 'Already A Member? Log-in'.

Fig. 3.6.1 Signing up Page



A screenshot of a web application's 'Login' page. The page has a red header bar with navigation links: 'SIGN UP', 'LOG-IN', 'PROJECT CONCEPT', and 'ABOUT US'. The main content area is light gray. On the left, there is a 6x6 color matrix. Below the matrix is a row of six colored squares: red, green, blue, yellow, purple, and white. On the right, there is a white card with the title 'Login'. Below the title are two input fields: 'User ID' and 'Virtual Password'. Below the password field are two red buttons: 'Login' and 'Refresh'.

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

R

G

B

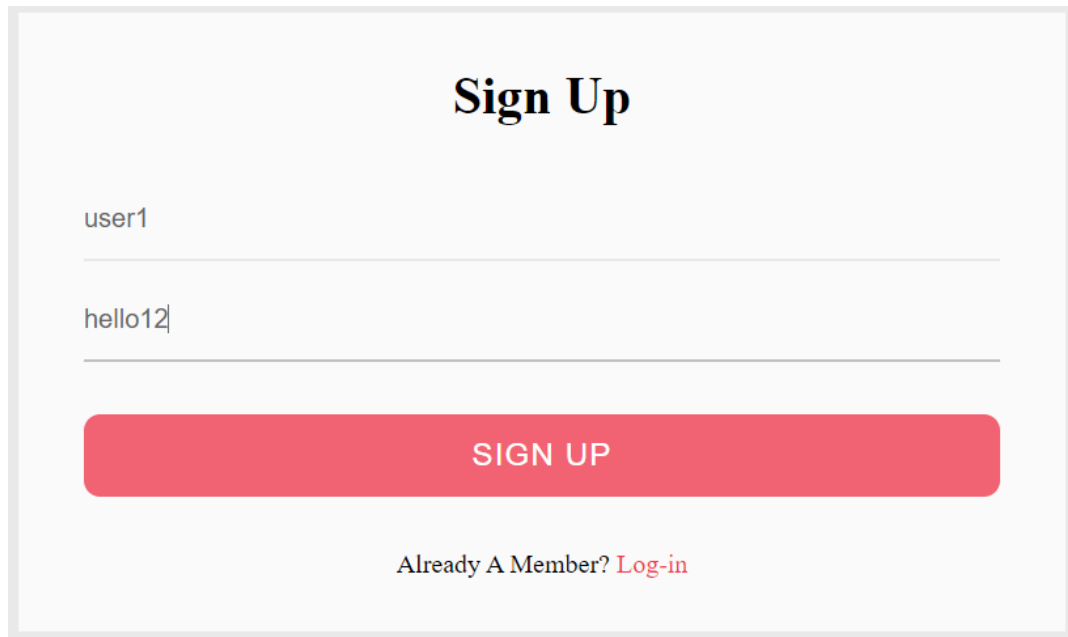
Y

P

W

Fig. 3.6.2 Login Page with color matrix

### I] Signing up with user name and actual password:



A sign-up form with a light gray background. At the top, the text "Sign Up" is centered in a large, bold, black serif font. Below it, there are two input fields. The first field contains the text "user1" and the second field contains "hello12". Both fields have a thin gray border. Below the input fields is a large, rounded rectangular button with a solid red background and the text "SIGN UP" in white, uppercase, sans-serif font. At the bottom of the form, the text "Already A Member? [Log-in](#)" is centered, with "Log-in" in red.

Fig 3.6.3 Sign up

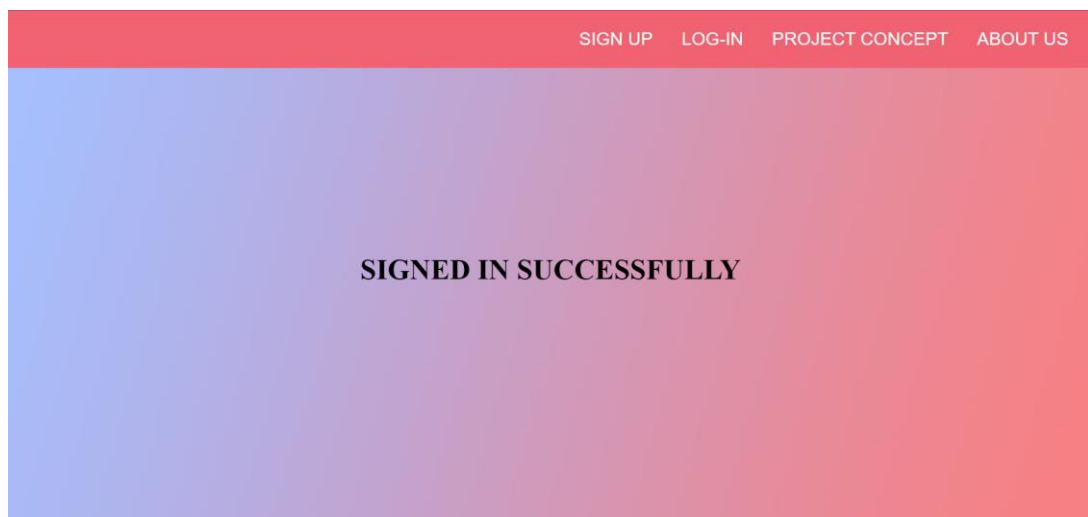


Fig 3.6.4 Successful Sign up



## II] Login in with virtual password using matrix:

Login using virtual password made of color initials {(R) r/ (G) g/ (B) b/ (Y) y/ (P) p/ (W)w}

The login interface consists of a 6x6 matrix and a virtual password sequence. The matrix is as follows:

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

Below the matrix is a sequence of colored boxes representing the virtual password: (R) (G) (B) (Y) (P) (W).

To the right of the matrix is a login form with the title "Login". It contains two input fields: "user1" and "gpyygww". Below the input fields are two buttons: "Login" and "Refresh".

Fig. 3.6.5 Login

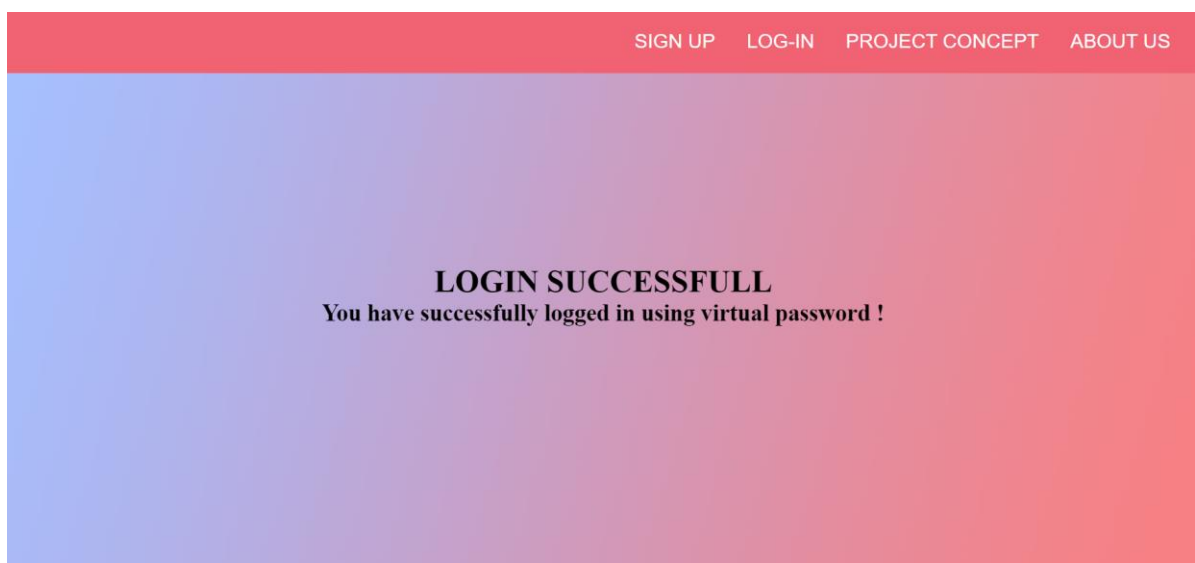


Fig. 3.6.6 Successfully logged in

### III] For unsuccessful login attempt:

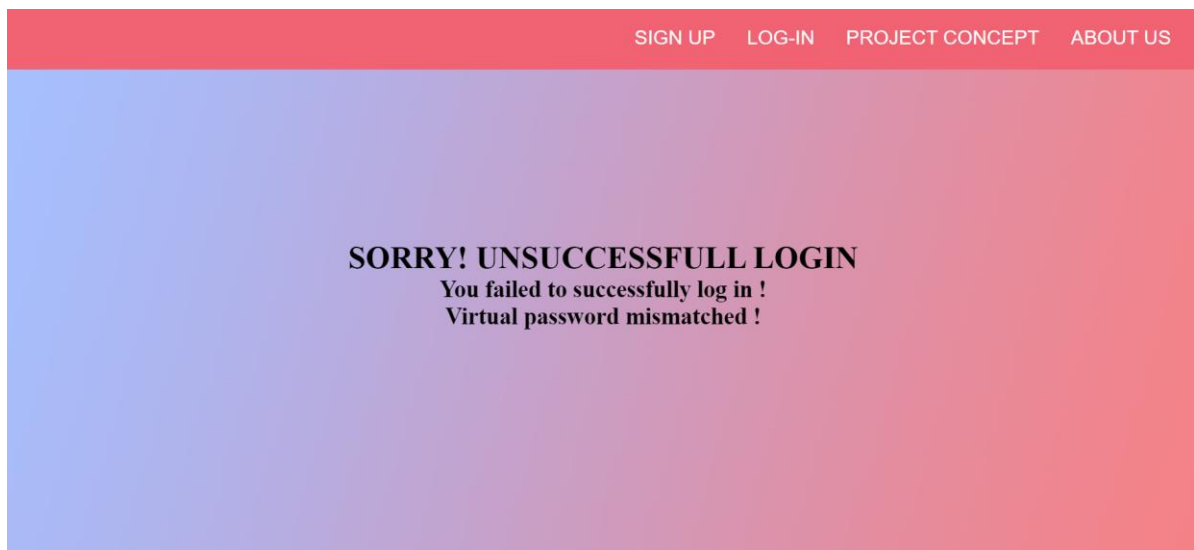


Fig. 3.6.7 Unsuccessful login attempt

### IV] New Login attempt or Refresh:

For a new login attempt or on refreshing old color matrix expires and new color mapping is shown:

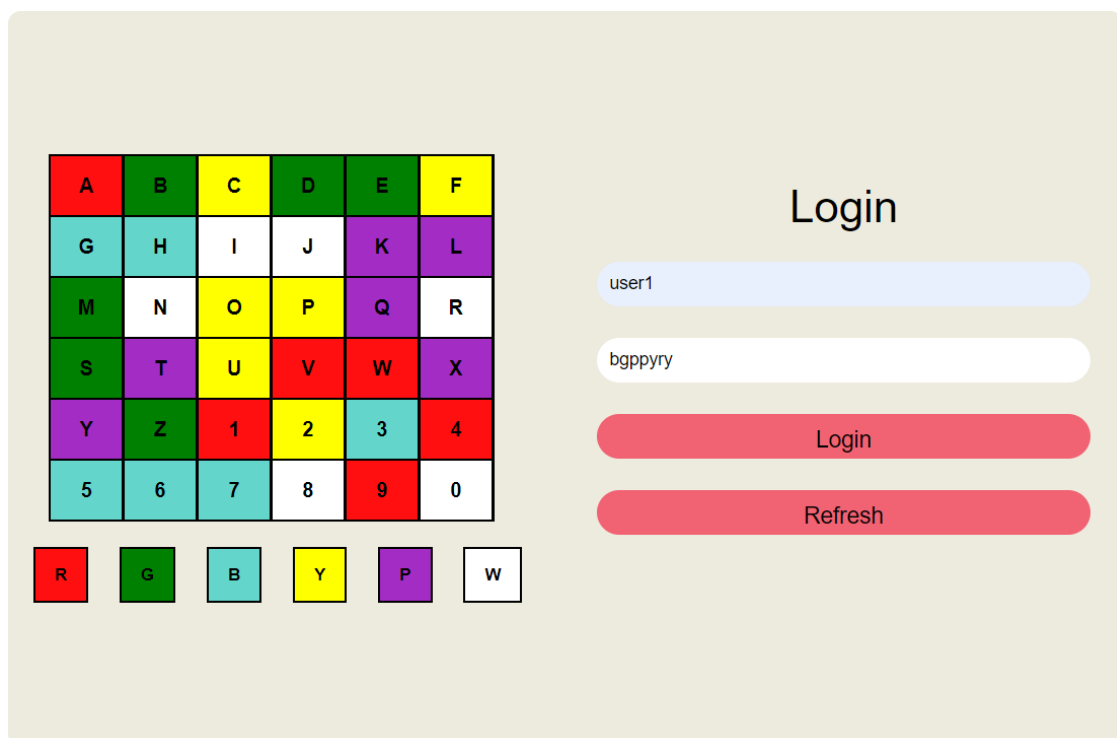


Fig. 3.6.8 New Login/Refresh

For earlier mapping as shown in Fig 3.6.5 virtual password was “**gpyygw**”, now for new

login virtual password for same user as shown above in Fig. 3.6.8 is “bgppry”.

## **4. SUMMARY AND CONCLUSION**

### **4.1 Summary:**

- As the reliance on technology for even our most basic of needs grows stronger by the day, it is essential to have a robust, reliable and intuitive system for protecting our data and finances. This stands true for both individuals as well as organizations.
- The Color Matrix based Virtual Password system is an application designed mainly with the goal of providing a simple, elegant, and intuitive way to lock applications, accounts and devices.
- The Color Matrix provides mapping for the characters which can be used in a password, such that each color is mapped to multiple characters. This ensures that any onlooker would be unable to figure out the correct password even if he learns the color pattern.
- The mapping of color matrix to characters is randomized at each login attempt, so that the correct pattern of colors to be entered changes with each login attempt.
- As the matrix is randomized at each attempt, any perpetrator would find it difficult to figure out the correct password pattern even after watching the user input the colors multiple times.
- This application provides a much more reliable and elegant solution to the problem of shoulder surfing attacks, even more so than the other contemporary technologies such as fingerprint scanning, face detection, pattern based locks, etc.

### **4.2 Conclusion:**

The Color Matrix based Virtual Password System is an application which builds on the fundamentals of the regular encryption based password systems currently in use to provide a novel and intuitive security system. It is mainly developed with the objective of reducing the threat of shoulder surfing attacks by adding an extra layer of protection over our regular passwords. The randomly generated color matrix ensures unique mapping at each login attempt, and the fact that multiple characters are mapped to

each color make it extremely difficult to obtain the correct password, even after multiple attempts of shoulder surfing.

## 5. LITERATURE CITED

- H. Gao, X. Guo, X. Chen, L. Wang and X. Liu, "YAGP: Yet Another Graphical Password Strategy," *2008 Annual Computer Security Applications Conference (ACSAC)*, 2008, pp. 121-129, doi: 10.1109/ACSAC.2008.19.
- H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing," *2010 International Conference on Cyberworlds*, 2010, pp. 194-199, doi: 10.1109/CW.2010.34.
- [https://www.researchgate.net/publication/224229789\\_A\\_graphical\\_password\\_authentication\\_system](https://www.researchgate.net/publication/224229789_A_graphical_password_authentication_system)
- AVI '06: Proceedings of the working conference on Advanced visual interfaces May 2006 Pages 177–184 <https://doi.org/10.1145/1133265.1133303>