

|| Jai Sri Gurudev ||

ADICHUNCHANAGIRI UNIVERSITY



A Mini Project Report On

“GRAPHICAL PASSWORD AUTHENTICATOR”

Submitted in partial fulfilment for the academic year 2023-24

Bachelor of Engineering

In

Artificial Intelligence And Machine Learning

Submitted by,

SHASHANK H L [21AME037]

SHASHANKA C K [21AME038]

Under the guidance of:
Mrs. AFSHA FIRDOSE
Asst.Professor,
Dept., of IS&E
BGSIT,BG Nagara



DEPARTMENT OF ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

B G S INSTITUTE OF TECHNOLOGY

B G NAGARA- 571448

2023-2024

||Jai Sri Gurudev||

ADICHUNCHANAGIRI UNIVERSITY
B G S INSTITUTE OF TECHNOLOGY
Department of Artificial Intelligence & Machine Learning
BG Nagara-571448, MANDYA



CERTIFICATE

This is to certify that the mini project entitled “**GRAPHICAL PASSWORD AUTHENTICATOR**” carried out by **Mr. SHASHANK H L**, bearing **USN: 21AME037** and **Mr. SHASHANKA C K**, bearing **USN:21AME038** of **BGS Institute OF Technology**, B.G Nagara in partial fulfilment for the award of Bachelor of Engineering in **Artificial Intelligence and Machine Learning** of Adichunchanagiri University during the year 2022-23. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the department library.

Signature of Guide

Signature of HOD

.....
Mrs. AFSHA FIRDOSE
Assistant Professor,
Dept., of IS&E
BGSIT., BG Nagar

.....
Dr. SIDDHARTHA B K
Associate Professor &
HOD, Dept. of AI&ML
BGSIT., BG Nagar

External Viva

Name of the Examiners

Signature with date

1. _____
2. _____

ACKNOWLEDGEMENT

We sincerely convey our regards and thanks to **Dr. Shobha B K , Principal, BGSIT, BG Nagar, Mandya**, for giving us a chance to carry out and present our mini project work.

Our sincere thanks to **Dr. Siddhartha B K, Prof. and Head of Department, AI&ML, BGSIT, B G Nagar, Mandya**, for giving us a chance to carry out and present our project work with all the support and facilities.

We would like to thank **Mrs. Afsha Firdose, Assistant Professor, Department of IS&E, BGSIT, BG Nagar** our honourable guides who stood as an excellent guide to carry out our work has been always available as an expressive evaluator for the creation and correction of the report towards our work. They have taken pain and time to go through our work when needed.

Our heartfelt gratitude to all the teaching and non-teaching faculties of **Artificial Intelligence And Machine Learning Department, BGSIT, BG Nagar, Mandya**, for their support and guidance towards the completion of our mini project work.

Finally, we would also extend our heartfelt thanks to our family members, classmates, friends and well-wishers for their support and encouragement throughout this effort.

SHASHANK H L (21AME037)

SHASHANKA C K (21AME038)

ABSTRACT

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area. We also try to answer two important questions: “Are graphical passwords as secure as text-based passwords?”; “What are the major design and implementation issues for graphical passwords”. In this paper, we are conducting a comprehensive survey of existing graphical image password authentication techniques. Also we are here proposing a new technique for graphical authentication.

CONTENTS

Title	Page No.
ACKNOWLEDGMENT	i
ABSTRACT	ii
CONTENTS	iii
LIST OF FIGURE	iv
CHAPTER 1 INTRODUCTION	1-5
1.1 Database	1
1.2 Database Management System	1-2
1.3 Applications	2
1.4 Introduction to MySQL	3
1.5 Oracle	4
1.6 Introduction to Project	5
CHAPTER 2 LITERATURE SURVEY	6
CHAPTER 3 PROBLEM STATEMENT	7-10
CHAPTER 4 REQUIREMENT SPECIFICATION	11-12
4.1 Hardware Requirements	11
4.2 Software Requirements	11
CHAPTER 5 IMPLEMENTATION	13-27
5.1 Implementation	5
5.2 Design	7
5.3 Source Code	14-17
5.4 ER Diagram	18
5.5 Schema Diagram	18
CHAPTER 6 SNAPSHOTS	19-20
CHAPTER 7 RESULT	21-22
7.1 Conclusion	21
7.2 Future Enhancement	21
7.3 References	22

LIST OF FIGURES

FIGURE.NO	FIGURE NAME	PAGE.NO
1.2	Database Management System	2
5.1	Home Page	19
5.2	Signup Page	19
5.3	Login Page	20
5.4	Inventory Page	20

CHAPTER 1

INTRODUCTION

1.1 Database

A database is an organized collection of data. A relation database, more restrictively, is a collection of schemas, tables, queries, report, views, and other elements. Database designers typically organize the data to model aspects of reality in a way that supports processes requiring information, such as modelling the availability of rooms in hotels in a way that supports finding a hotel with vacancies.

A database is not generally portable across different DBMS, but different DBMSs can interoperate by using standards such as SQL and JDBC to allow a single application to work with more than one DBMS. Computer scientists may classify database management system according to the data base models that they support; the most popular database systems since the 1980s have all supported the relational model- generally associated with the SQL language. HB sometimes a DBMS is loosely referred to as a “database”.

1.2 Database Management System

A database-management system (DBMS) is a collection of interrelated data and a set of programs to access those data. This is a collection of related data with an implicit meaning and hence is a database. The collection of data, usually referred to as the database, contains information relevant to an enterprise. The primary goal of a DBMS is to provide a way to store and retrieve database information that is both convenient and efficient. By data, we mean known facts that can be recorded and that have implicit meaning. For example, consider the names, phone numbers, addresses, age of the person you know. You may have recorded this data in an indexed address book, or you may have stored it on a diskette, using a personal computer and software such as DBASE IV or V, Microsoft ACCESS, or EXCEL. While information can be transported, stored or shared without many difficulties the same cannot be said about knowledge.

Database system are designed to manage large bodies of information management of data involves both defining structures for storage of information and providing mechanisms for the manipulation of information. In addition, the database system must ensure the safety of the information stored, despite system crashes or attempts at unauthorized access. If data are to be shared among several users, the system must avoid possible anomalous results.

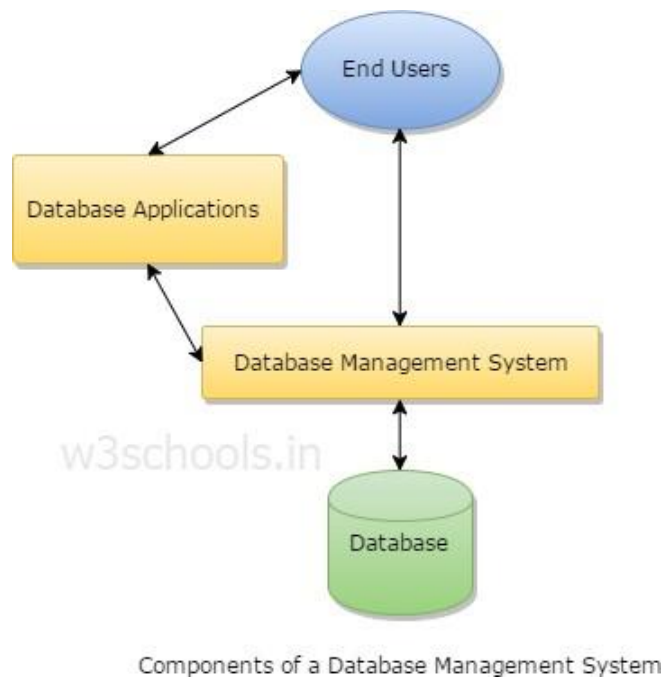


Figure:1.2 Database Management System

1.3 Application

Database are widely used some of the representative applications are:

1. **Banking:** For Customer Information, Accounts and Loans and Banking Transactions.
2. **Universities:** For Student Registration and Grades.
3. **Online Shopping:** Everyone Wants to Shop from Home. Everyone New Products Are Added and Sold Only with The Help Of DBMS. Purchase Information, Invoice Bills and Payment, all of these Are Done with The Help Of DBMS.

4. **Airlines:** For Reservation and Schedule Information.
5. **Credit Card Transactions:** For Purchases on Credit Cards and Generation of Monthly Statements.
6. **Library Management System:** Maintain All the Information Related to The Book Issue Dates, Name of The Book, Author and Availability of The Book.
7. **Telecommunication:** For Keeping Records of Call Made, Generating Monthly Bills, Maintaining Balances on Prepaid Calling Cards.
8. **Sales:** For Customer, Products and Purchase Information.
9. **Finance:** For Storing Information About Holdings, Sales, And Purchases of Financial Instruments Such as Stocks and Bonds.

1.4 Introduction to MySQL

MySQL Is a Relational Database Management System (RDBMS) That Runs as A Server Providing Multi-User Access to A Number of Databases. MySQL Is a Popular Choice of a Database for Use in the Web Applications and Is an Open-Source Product. The Process of the Setting Up a MySQL Database Varies from Host to Host, However We Will End Up with a Database Name, A User Name and a Password. Before Using Our Database, We Must Create a Table. A Table Is a Section of The Database for Storing Related Information. In A Table, We Will Set Up Different Fields Which Will Be Used in that Table. Creating a Table. In PhpMyAdmin Is Simple, We Just Type the Name, Select the Number of Fields and Click on the 'go' Button. We Will Then Be Taken to a Setup Screen Where You Must Create the Fields for The Database. Another Way of Creating Database and Tables in PhpMyAdmin Is by Executing Simple SQL Statements. We Have This Method in Order to Create Our Database and Tables. RDBMS is the basis for SQL, and for all modern database systems such as MS SQL Server, IBM DB2, Oracle, MySQL, and Microsoft Access.

The most comprehensive set of advanced features, management tools and technical support to achieve the highest levels of MySQL scalability, security, reliability, and uptime. Over 2000 ISVs, OEMs, and VARs rely on MySQL as their products' embedded database to make their applications, hardware and appliances more competitive, bring them to

market faster, and lower their cost of goods sold. SQL is used to communicate with the database. According to ANSI (American National Standard Institute), it is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. It is also used by business professionals or program developers for administering, updating, maintaining and manipulating the databases are tables that used for business decision-making

1.5 Oracle

Popular Choice of Database for Use in Web Applications and Is an Open-Source Product. The Process of Setting Up a MySQL Database Varies from Host to Host, However We Will End Up with A Database Name, A User Name and A Password. Before Using Our Database, We Must Create a Table. In A Table, We Will Set Up Different Fields Which Will Be Used in That Table. Creating A Table in PhpMyAdmin Is Simple, We Just Type the Name, Select the Number of Fields and Click The ' Go' Button. We Will Then Be Taken to A Setup Screen Where You Must Create the Fields for The Database. Another Way of Creating Database and Tables in PhpMyAdmin Is by Executing Simple SQL Statements. We Have This Method in Order to Create Our Database and Tables.

The Current Version of The Oracle Database Is the Result Of 30 Years of Innovative Development. Highlights In the Evolution of Oracle Database Include the Following:

- **Founding Of Oracle**

In 1977, Larry Ellison, Bob Miner, And Ed Oates Started the Consultancy Software Development Laboratories, Which Became Relational Software, Inc. (RSI). In 1983, RSI Became Oracle Systems Corporation and Then Oracle Corporation.

- **First Commercially Available RDBMS**

In 1979, RSI Introduced Oracle V2 (Version 2) As the First Commercially Available SQL Based RDBMS, A Landmark Event in The History of Relational Databases.

- **Portable Version of Oracle Database**

Oracle Version 3, Released In 1983, Was the First Relational Databases to Run on Mainframes, Minicomputers and PCs. The Database Was Written In C, Enabling the Database to Be Ported to Multiple Platforms.

Version 4 introduced Multi Version Read Consistency Version 5, Released In1985, Supported Client/Server Computing and Distributed Database System Version 6 Brought Enhancements to Disk I/O, Row Locking, Scalability and Backup and Recovery. Also, Version 6 Introduced the First Version of the PL/SQL Language, A Proprietary Procedural Extension To SQL.

1.6 Introduction to Project

Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in Graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

CHAPTER 2

LITERATURE SURVEY

Related work:

Cyberattacks have been rising exponentially since the past decade. Data is very precious today than it ever had been. This data ranges from a user's personal data to a country's highly confidential data. This data must be protected from going into wrong hands at all costs. Cyber criminals use various methods to gain illegal access and steal this data, some of the most common methods being phishing/social engineering, compromised/stolen devices and credential theft. Passwords are one of the ways to authenticate users who have the rights to create, access, modify or delete the data. Traditional passwords consist of a string of alphanumeric characters of varying length. One of the challenges of using such passwords is that, users tend to forget them. According to a study, 78% of users forget their passwords and go for reset. Some of the methods that users resort to overcome this challenge are to write down the password somewhere or set an easy password. Easy to remember passwords are also prone to brute-force and dictionary attacks. A study conducted by Avast – a multinational cybersecurity software company, shows that 83% of the users in the United States apply weak passwords.

Phishing attacks where an attacker asks for user's credentials by posing as a legitimate website or application can also be carried out for alphanumeric passwords. Research conducted by various institutions show that human brain has a greater capability to remember what they see. This gives rise to an idea that graphical passwords are easier to remember than traditional alphanumeric passwords. So, to overcome the limitations of alphanumeric passwords, we introduced a Graphical Password Authentication System. The proposed system uses a random set of images from which the users select some of them in a specific order to form the password. Such a password is easier to remember and more secure than the traditional alphanumeric passwords.

CHAPTER 3

PROBLEM STATEMENT

3.1 Existing System

In traditional authentication systems, alphanumeric passwords are commonly used to secure user accounts. However, these passwords are susceptible to various security threats such as brute-force attacks, phishing, and password reuse. To address these vulnerabilities and enhance the overall security of user authentication, there is a need for innovative and more secure authentication methods.

DRAWBACKS OF EXISTING SYSTEM

1. Password Weakness:

- Users often choose weak passwords that are easy to guess or are common words.
- Lack of complexity, such as the absence of special characters or a mix of uppercase and lowercase letters, makes passwords susceptible to brute-force attacks.

2. Password Reuse:

- Many users reuse the same password across multiple accounts, increasing the risk of a security breach if one account is compromised.
- Password reuse is common due to the challenge of remembering multiple complex passwords.

3. Lack of Two-Factor Authentication (2FA):

- Many traditional password systems lack the additional layer of security provided by two-factor authentication.
- Relying solely on passwords makes accounts more vulnerable to

unauthorized access.

4. Limited User Authentication Methods:

- Traditional alphanumeric passwords offer a limited range of authentication methods and may not leverage the full spectrum of user cognitive abilities.

3.2 PROPOSED SYSTEM

In traditional authentication systems, alphanumeric passwords are commonly used to secure user accounts. However, these passwords are susceptible to various security threats such as brute-force attacks, phishing, and password reuse. To address these vulnerabilities and enhance the overall security of user authentication, there is a need for innovative and more secure authentication methods.

Graphical passwords present a promising alternative, leveraging users' visual memory and cognitive abilities to create a more robust authentication process. The problem lies in designing and implementing an effective Graphical Password Authenticator that balances usability, security, and resistance to attacks.

ADVANTAGES

- **Usability and Memorability:**

Designing a graphical password system that is intuitive for users with varying levels of technical expertise.

Ensuring that users can easily create and remember their graphical passwords without compromising security.

- **Security:**

Developing mechanisms to prevent common graphical password attacks such as shoulder surfing, smudge attacks, and pattern analysis.

Evaluating the system's resistance to brute-force attacks and other potential security threats.

- **Accessibility:**

Ensuring that the graphical password authentication system is accessible to users with disabilities.

Addressing potential challenges related to colour blindness, visual impairments, and

other accessibility considerations.

- **Authentication Recovery:**

Implementing a secure and user-friendly method for users to recover their accounts in case they forget their graphical passwords.

Balancing the need for account recovery with the system's overall security.

- **Integration and Compatibility:**

Integrating the graphical password authentication system with existing authentication frameworks and protocols.

Ensuring compatibility across different devices and platforms.

- **User Acceptance and Education:**

Overcoming potential resistance from users unfamiliar with graphical password systems.

Developing educational materials and training programs to help users understand and adopt the new authentication method.

CHAPTER 4

REQUIREMENTS SPECIFICATION

4.1 Hardware Requirements

The Physical Components Required Are:

- Processor- Intel Pentium Processor At 500 MHz Or Faster.
- Memory- 256MB RAM or More.
- Wi-Fi Card OR Ethernet Card.
- Mouses Or Others Pointing Device.
- Keyboard
- Hard-Disk Drive/Optical Driver.

4.2 Software Requirements

The softer being used are:

- Operating system (ex: windows 10)
- Xampp server
- Subline text editor
- Internet browser (ex: chrome).

4.3 REQUIREMENTS

4.3.1 Frontend

Introduction to visual basic

Visual basic is most popular programming language in the world, and generally use as a front end for database application. There are some important reasons to use visual basic

rather than others. Capability, flexibility, familiarity, popularity. The “visual” part refers to the method used to create the graphical user interface (GUI).

4.3.2 Back end

Introduction to MYSQL server

MYSQL is a relational database management system. A relational database stores data in separate tables rather than putting all the data in one big storeroom. This adds speed and flexibility. The SQL is part of MYSQL stand for “structured query language”.

4.3.3 Case tool

Introduction to case tool

This is a brief overview to get students started in using rational rose to quickly create object-oriented models and diagrams. It is not by any means a complete introduction to rational rose, but it should get you started.

- Getting started
- Use case diagram

CHAPTER 5

IMPLEMENTATION

5.1 MODULES

The system has various modules:

- Admin
- Login
- Feedback

5.1.1 Admin:

The admin will perform various function.

- Display the summary
- Manage Password. Such as (Alphanumeric, Graphical)
- Category Management (Update Password, delete Password)
- Reports
- Manage user list, manage account details/credentials, Manage system information

5.1.2 Login:

The login will perform various functions.

- create new user by registering.
- Allows user to fetch the details from database for logging next time.
- After the registration the users can view their profile.

Code For Admin:

```
-- phpMyAdmin SQL Dump

-- version 4.8.0
-- https://www.phpmyadmin.net/
--
-- Host: 127.0.0.1
-- Generation Time: Apr 20, 2019 at 08:47 PM
-- Server version: 10.1.31-MariaDB
-- PHP Version: 7.2.4

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET AUTOCOMMIT = 0;
START TRANSACTION;
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

-- Database: `gpas_final`
-- Table structure for table `user`
CREATE TABLE `user` (
  `username` varchar(80) NOT NULL,
  `password` varchar(80) NOT NULL,
  `name` varchar(80) NOT NULL,
  `email` varchar(80) NOT NULL,
  `phone` bigint(10) NOT NULL,
  `userimage` varchar(800) NOT NULL,
  `image1` varchar(800) NOT NULL,
  `slice1` int(1) NOT NULL,
```

```
`image2` varchar(800) NOT NULL,  
`slice2` int(1) NOT NULL,  
`image3` varchar(800) NOT NULL,  
`slice3` int(1) NOT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=latin1;  
-- Indexes for dumped tables  
-- Indexes for table `user`  
ALTER TABLE `user`  
  ADD PRIMARY KEY (`username`,`email`,`phone`);  
COMMIT;  
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;  
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;  
/*!40101 SET COLLATION_  
CONNECTION=@OLD_COLLATION_CONNECTION */;
```

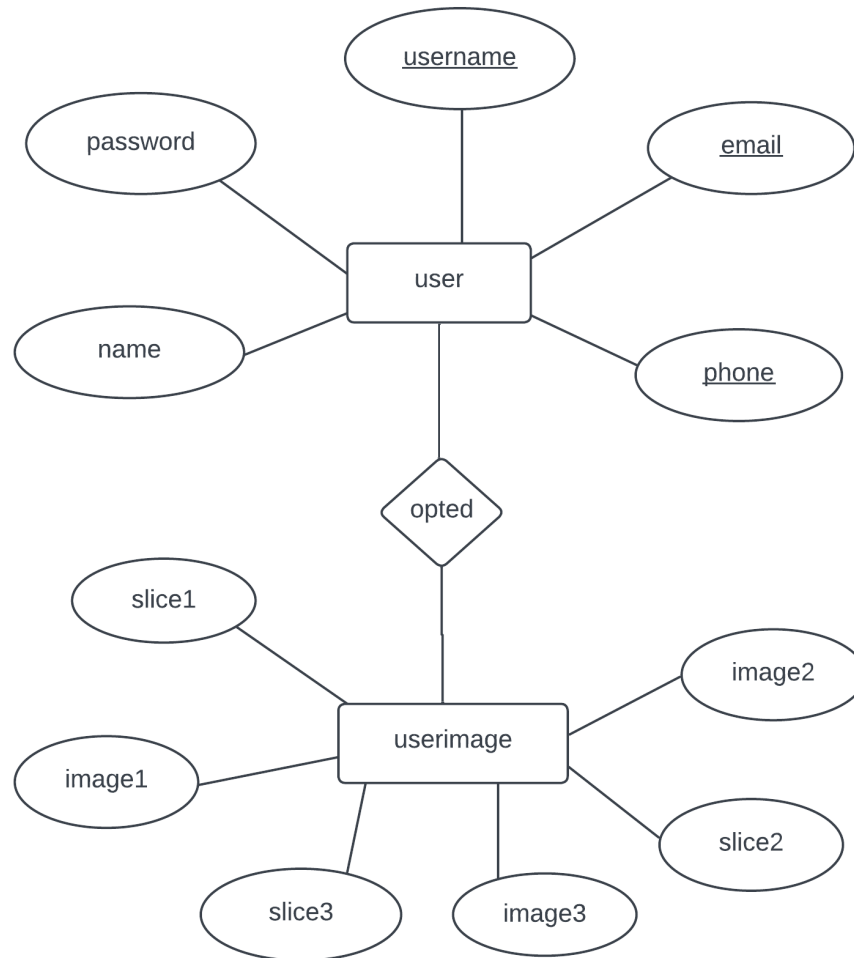
Code For Login:

```
<?php
session_start();
session_destroy();
session_start();
ob_start();
include("db.php");
if(!isset($_SESSION))
{
    session_start();
}
$name=$_POST['name'];
$password=$_POST['password'];
$password=md5($password);
$query="select * from user where username='$name' and password='$password'";
$result=mysqli_query($con,$query);
if($result)
{
    $rows=mysqli_num_rows($result);
    if($rows>0)
    {
        $row=mysqli_fetch_array($result);
        $_SESSION['uname']=$name;
        header('Location:log_img1.php');

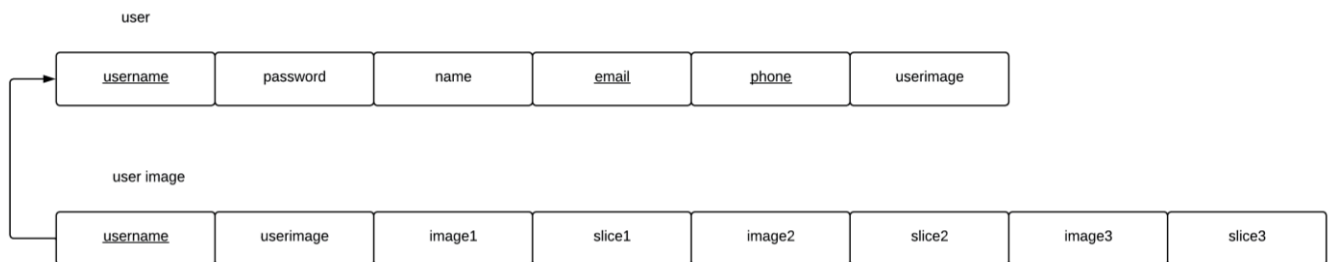
    }
    else
    {
        $query="select * from user where username='$name' and password='$password'";
    }
}
$result=mysqli_query($con,$query);
```

```
$row=mysqli_fetch_array($result);  
$rows=mysqli_num_rows($result);  
if($rows==0)  
    header('Location:invalid_textpw.html');  
}  
}  
?>
```

5.4 ER Diagram



5.5 Schema Diagram



CHAPTER 6

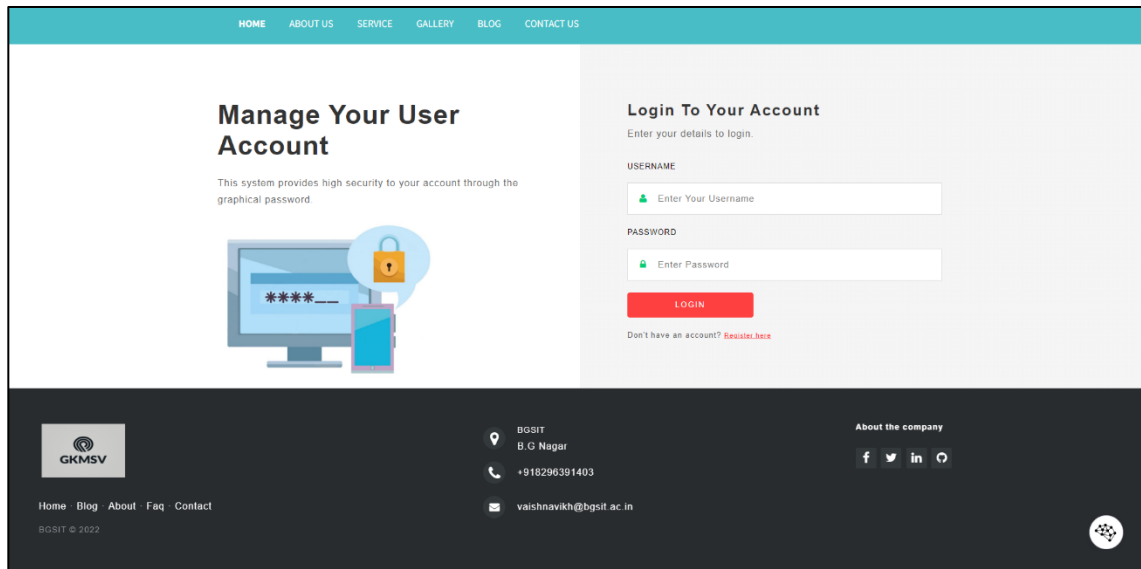
SNAPSHOT



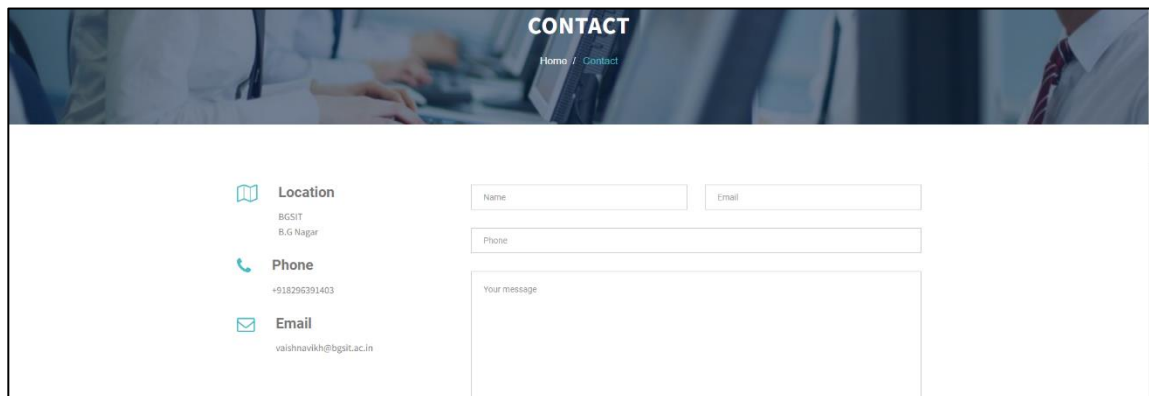
Fig 6.1 Home Page.

The screenshot shows the signup page of the Graphical Password Authentication System. The header includes the navigation bar with links: HOME, ABOUT US, SERVICE, GALLERY, BLOG, and CONTACT US. The main content area is divided into two sections. The left section, titled "Manage Your User Account", includes a sub-header "Manage Your User Account" and a description: "This system provides high security to your account through the graphical password." Below this is an illustration of a computer monitor and a smartphone, both displaying a graphical password (a grid of dots). The right section, titled "Create New Account", includes a sub-header "Create New Account" and a description: "Enter your details to create the account." Below this are three input fields: "USERNAME" (with a placeholder "Enter Your Username"), "PASSWORD" (with a placeholder "Enter Your Password"), and "RE-ENTER PASSWORD" (with a placeholder "Enter Your Password Again").

Fig 6.2 Signup Page.



The screenshot shows a web application interface for a graphical password authenticator. The top navigation bar is teal and contains links: HOME, ABOUT US, SERVICE, GALLERY, BLOG, and CONTACT US. The main content area is divided into two sections. The left section, titled "Manage Your User Account", features a sub-header "This system provides high security to your account through the graphical password" and an illustration of a computer monitor and a smartphone, both displaying a graphical password interface. The right section, titled "Login To Your Account", prompts the user to "Enter your details to login." and includes input fields for "USERNAME" and "PASSWORD", each with a green eye icon for toggling visibility. A red "LOGIN" button is positioned below the password field. A link "Don't have an account? Register here" is located at the bottom of the login section. The footer is dark grey and contains the GKMSV logo, contact information (BGSIT, B.G. Nagar, +918296391403, vaishnavikh@bgsit.ac.in), social media icons (Facebook, Twitter, LinkedIn, YouTube), and a copyright notice "BGSIT © 2022".

Fig 6.3 Login Page

The screenshot displays a "CONTACT" page with a header image showing hands typing on a laptop. The page includes a breadcrumb trail "Home / Contact". On the left, contact details are listed: "Location" (BGSIT, B.G. Nagar), "Phone" (+918296391403), and "Email" (vaishnavikh@bgsit.ac.in). On the right, there is a contact form with input fields for "Name", "Email", and "Phone", and a larger text area for "Your message".

Fig 6.4 Inventory Page.

CHAPTER 7

RESULT

7.1 CONCLUSION

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In future development we can also add challenge response interaction. In challenge-response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Also, we can limit the number a user can enter the wrong password

7.2 FUTURE ENHANCEMENT

In future it has great scope. It can be used everywhere instead of text-based password. We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication system but they have their own advantages and disadvantages. Text password can be hacked easily with various methods where as biometric authentication can cause more cost. This system is more secure and cheap than old methodologies. As well as this system allows more reliable and easily recognizable system to the users. As how we have written over this system can be best alternative to the text password.

7.3 REFERENCES

- [1] <https://www.python.org/doc/>
- [2] <https://www.djangoproject.com/>
- [3] <https://Youtube.com/>
- [4] Wikipedia.org/
- [5] www.w3schools.com/