Engineering and Technology Journal e-ISSN: 2456-3358
Volume 08 Issue 07 July-2023, Page No.- 2417-2421
DOI: 10.47191/etj/v8i7.06, I.F. – 7.136

A Colour Scheme Authenticated Tutor Booking Website

Oke A. O.[1], Ogbewey L. I.[2], Oguntoye J. P.[3], Jubril A. A.[4], Shokenu E. S.[5]
[1,3,5]Department of Computer Engineering, Ladoke Akintola University of Technology, P.M.B. 4000, Ogbomoso, Oyo State.
[2]Department of Computer Engineering, Federal Polytechnic Offa, Kwara State.
[4]Department of Computer Engineering, Auchi Polytechnic Auchi, Edo State

ABSTRACT: Authentication is the first and most important step in information security. Traditional password authentication systems are not strong enough to cope with the current age of cybercrime because passwords can be easily predicted by attackers. This paper aims at reducing threats from different malicious activities to a great extent, thereby increasing security and efficiency, proving it to be very advantageous in today's world where confidential data security has become so essential. This system provides users with the freedom to have complete security while handling their confidential data and security essential systems from anywhere.
The colour code authentication scheme is executed using colour features for passwords, where users have to select a colour code as password item in terms of the uniqueness and reliability with which it can be entered. This technique uses a grid for session passwords generation and is resistant to dictionary attacks, brute force attacks, and shoulder-surfing. The colour scheme allocated ratings to colours, based on these ratings and the grid displayed during login, session passwords were generated. This work explored a new and easy password authentication system devoid of memorization and recall. This authentication system makes data more secure as only the colour rating at the registration phase needs to be remembered. The Colour based authentication system would provide an efficient way to encrypt account details for sensitive applications such as defense and banking

KEYWORDS: Authentication, Security, Password, Colour Scheme, Tutor Booking, Encryption.

1. INTRODUCTION

Authentication is a process that ensures and confirms a user's identity (Munir and Mohammed, 2019). In today's high technology environment, organizations are becoming more dependent on information systems. The public is increasingly concerned about the proper use of information, particularly personal data while threats to information systems from criminals and terrorists are increasing [8]. Studies have shown that users tend to pick short passwords or passwords that cannot be forgotten [3]. Both Textual, graphical passwords have issues of hacking and cloning; also, Graphical passwords have disadvantages [2].

Despite extensive usage, passwords and PINs have several shortcomings. Simple or meaningful passwords are easier to remember and, at the same time, vulnerable to attacks [1]. Complicated passwords are difficult to remember, while the biometric seems to be more expensive and makes use of an additional component [5]. The best solution is to provide an authentication scheme that provides higher security and higher efficiency than the existing system [9].

Web applications have aided in restructuring most of the tasks performed every day, which makes lives simple and uncomplicated. This describes the importance of Information and Communication Technology in improving and assisting teaching and learning processes [6]. These applications are most widely used in solving problems concerning student learning and scheduling appointments. To eliminate these human errors due to manual appointments scheduling system, there is need to develop a web application that makes appointment processes easier [10].

The proposed system provides higher security against various attacks by using both colours and numbers as a means of authentication and verification. The login interface has the colour grid and number grid of eight rows and eight columns, having numbers one to eight (1 - 8) randomly placed in the grid. This scheme authenticates users by session passwords. Session passwords are passwords that are used only once [7] and are gotten depending on the ratings given to colours. The number in the intersection of the row and column of the grid is part of the session password. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication scheme uses text and colours for generating session passwords.

2. SYSTEM DESIGN OVERVIEW

The design of the online tutor booking system was achieved by designing a database using conceptual, logical and physical database design. These were developed using tools Microsoft Visio and Sublime text. Microsoft project professional a project management tool was used to present the time schedules for the

system development procedures, task dissemination and ordering.

- **LOGICAL DESIGN**

Logical design of a system pertains to an abstract representation of the data-flows, inputs and outputs of the system. This is often conducted via modeling using an over-abstract and sometimes graphical model of the actual system. The graphical user interface displays the input design, required data-type for inputs and the output design. Also, a careful study of the flowchart showed the logical steps by which the system achieves its goals and procedures. This is called the logical design.

- **PHYSICAL DESIGN**

The physical design relates to the actual input and output processes of the system. This shows how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed as in physical design.

- **INPUT/OUTPUT DESIGN.**

Format and specification input medium was used by the system for data entry by the keyboard and some data can be obtained from files stored in CDs and flash drives. The variable to the input design were name, sex, email, program and course.

DATA FLOW DIAGRAM (DFD)

Data flow diagram shows the flow of data from external entities into the system, and from one process to another within the system. There are four symbols for drawing a DFD:

1. Rectangles representing external entities, which are sources or destinations of data.
2. Ellipses representing processes, which take data as input, validate and process it and output it.
3. Arrows representing the data flows, which can either, be electronic data or physical items
4. Open-ended rectangles or a Disk symbol representing data stores, including electronic stores such as databases or XML files and physical stores such as filing cabinets.

Figure 1 is a Context Level Diagram (parent) which shows the processes in which users (parent/guardians) have to pass before booking a tutor for wards. New user (parent/guardians) needs to register before the website can be accessed while existing user needs to login using email and password. After which the user (parent/guardian) interact with the website, by selecting tutors for the desired subjects, making payment for the selected tutors time, and by booking tutor. Context Level Diagram (tutor) are processes in which users (tutor) go through before students around the tutor area can access and be tutored. New user (tutor) needs to register before such can access the website while existing user need to login using phone number, email and password the process is shown in Figure 2.

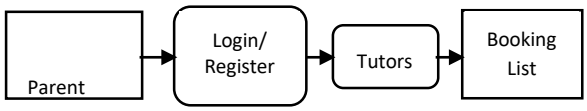

Figure 1. Context Level Diagram (Parent)

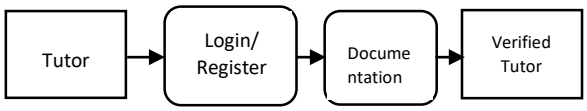

Figure 2. Context Level Diagram (tutor)

Context Level Diagram (admin) are processes in which admin have to pass through before backend can be edited. Admin needs to login using the username and the password (colour code), the process is shown in Figure 3. Admin page being secured by the colour code authenticated scheme is login by username and the assigned colour. The admin page shows how the admin interact with the website, by adding new subjects, verification of tutors, adding of new location, reviews of booking history. Second level DFD (parent) as shown in Figure 4 display how Parent and guardians interact with the website, by selecting tutors for the desired subjects that the ward needs, making payment for the selected tutors time, and booking the tutor. Second level DFD (tutor) shows how tutors interact with the website, by uploading the required document for final verification.

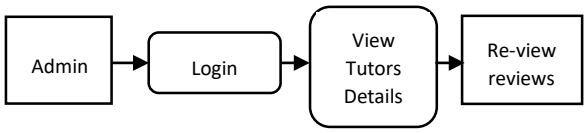

Figure 3. Context Level Diagram (admin)

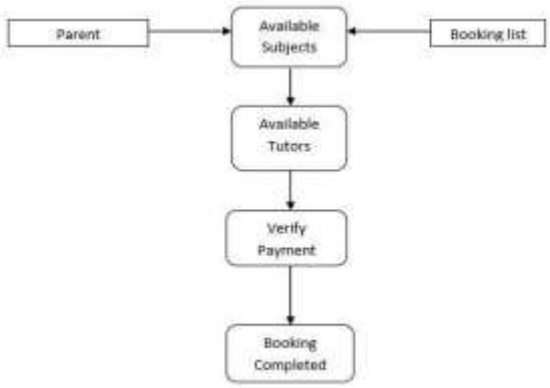

Figure 4. Second Level DFD (parent)

Once verified, the tutor becomes accessible as shown in Figure 5. Second level DFD (admin) shows how admin interact with the website, by adding new subject and removing subjects that

have no verified tutors, by removing tutors that have bad reviews, verification of tutors, adding of new location, as shown in Figure 6. The Context Level DFD provides a conceptual view of the process and its surrounding input, output and data stores. The detailed DFD provides a more detailed and comprehensive view of the interaction among the subprocesses within the system.

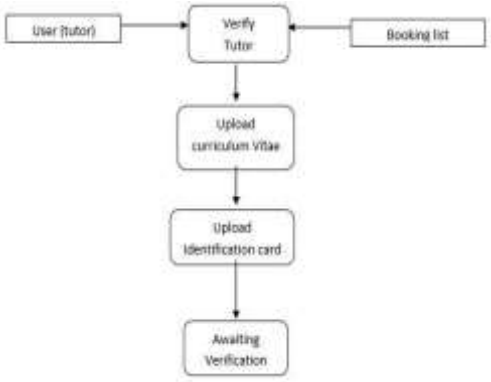

Figure 5. Second Level DFD (Tutor)

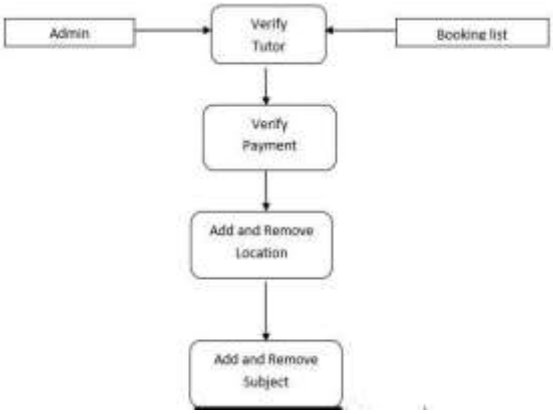

Figure 6. Second Level DFD (Admin)

3. SYSTEM OPERATION

A. Colour Authenticated Admin Page

This is the page where the colour scheme authentication is executed and all the activities done on the website is controlled, it is accessed with the colour code combination pass code as shown in Figure 7, the colour code authentication scheme prevents it from hacking and shoulder surfing attack while it ensures that the tutor and students' details are safe. There are six main security features that are used on existing graphical password schemes.

The possible attack method is not classified as the security feature, it is only for the guidance and supporting reason of why the security feature needed. The possible attack method is divided into six types of attacks which are brute force, dictionary, guessing, spyware, shoulder-surfing and social engineering. These are the current active attack methods in graphical authentication environment.

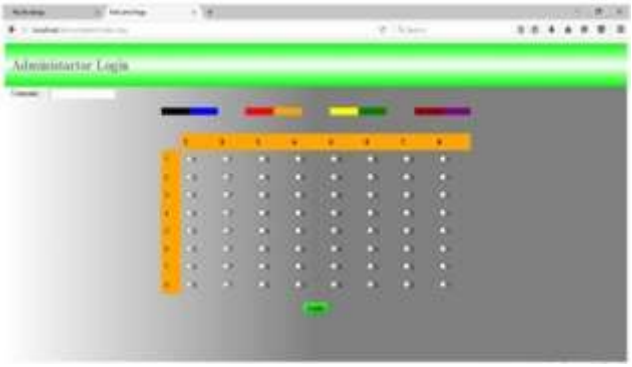

Figure 7. Administrative login page

The software was executed with ten participants as students and seven participants as tutors. Being a new technique, the participants were briefed about the techniques. Demonstrations were given for better understanding. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions. The sessions were conducted within the time frame of one week.

- **The admin login page**

The design source code of the admin login page is shown. It is displayed when an authorized admin tries to access the page of the application. It is accessed using colour code combination.

```
session_start();
  if (!isset($_SESSION['username'])) {
                              header('location: index.php');
          }
          echo $_SESSION['username'];
          ?>
```

B. Home Page Login

The home page source code of this website is shown. It's the page of the website where the choice of the type of user is been chosen. Either becoming a tutor or book a tutor as the case may be.

```
<?php
    $dbuser="root";
    $dbpass="";
    $host="localhost";
    $mysqli = new mysqli
    ($host,$dbuser,$dbpass, $db);
    $config->title = "Tutor";
    $config->about = " We are professionals in providing
    a competent tutor that is nearby for your children. We
    have different tutors available in different subject
    available to be booked";
?>
```

C. User Login Page

The design source code for the user page is shown. The user login page represents the login form where a user can enter and submit credentials for authentication purpose. It is displayed

whenever the user tries to access the page. If authorization fails, an error message is displayed.

```
<?php session_start(); include('../powerhouse/config.php');
if(isset($_POST['login']))
{
$email=mysqli_real_escape_string
($mysqli,$_POST['email']);
$password=mysqli_real_escape_string
($mysqli,$_POST['password']);
$password = md5($password);
$stmt=$mysqli->prepare
("SELECT email,password,id FROM users WHERE
email=? and password=? ");
$stmt->bind_param('ss',$email,$password);
$stmt->execute();
$stmt -> bind_result
($email,$password,$id); $rs=$stmt->fetch();
$stmt->close();
$_SESSION['email']=$email;
$_SESSION['login']=$email;
$uip=$_SERVER['REMOTE_ADDR'];
$ldate=date('d/m/Y h:i:s', time()); if($rs)
{
$uid=$_SESSION['email'];
$uemail=$_SESSION['login'];
$ip=$_SERVER['REMOTE_ADDR'];
$geopluginURL='http://www.geoplugin.net/php.g
p?ip='.$ip; $addrDetailsArr = unserialize
(file_get_contents($geopluginURL));
$city = $addrDetailsArr['geoplugin_city'];
$country =$addrDetailsArr
['geoplugin_countryName'];
$log="insert intouserLog
(userId,userEmail,userIp,city,country
values('$uid','$uemail','$ip','$city','$country')";
$mysqli->query($log); if($log)
{
header("location:index.php");
}
}else
{
echo "<script>alert('Invalid Email or
password');</script>";
}
}
?>
```

4. RESULTS AND DISCUSSION

The results from the written program used in the methodology produced a tutor booking website. It is an effective online tutor booking system designed carefully to make life simple and stress-free by letting students pay for tutoring appointments online. Booking online tutoring lessons gained considerable popularity in the past several years. It is not surprising that many parents are now choosing online tutoring lessons booking over conventional ways of tutoring admission at a learning center.

The results of this online tutor booking website are shown in Figures 8 to 10. The home page is as shown in Figure 8 and the entry point is to click the "Become A Tutor" button. When "Become A tutor" is clicked, a new page which is the Tutor Login page pops up where returning user can login and new user can register. Students that want to register for lesson would click the "book a tutor" button on the top right corner of the website. A new user is required to provide the necessary information as shown in Figure 9 and a verification procedure would be followed as shown in Figure 10. The verification was completed within a time frame from the date of the updated details. Once the details were updated, details uploaded successfully and awaiting verification would pop up.

Figure 8. Tutor Registration

Figure 9. Tutor Login Page

Figure 10. Tutors Panel

5. CONCLUSION

System using a session password provides much security. Authentication using the colour system can be used where

security is very significant, such as bank, security outfits etc. Such a system can be used to protect significant data. Users can easily and efficiently login the system. This work, therefore, can be adopted by individuals, firms and governments that wish to use a better website authentication method, the shopping sites can also adopt this authentication scheme for improving site security. Besides, this scheme can be used in any other application where security is the main concern.

There is a growing interest for graphical passwords since it is better than text-based passwords, as the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. This technique is easy and offers resistance to existing possible attacks, especially shoulder surfing, screen capture, or man in the middle attacks. The usability of an authentication scheme as well as its security is of prime importance, the proposed method would provide an efficient authentication system.

REFERENCES

1. Asraful Haque, Babbar Imam, (2014) "A New Graphical Password: Combination of Recall and Recognition Based Approach", World Academy of Science Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol: 8 No: 2.
2. Blonder G. E. (1996) "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States.
3. Davis D., Monrose F., and Reiter M. K., (2004) "On user choice in graphical password schemes," in Proc. 13th USENIX Security Symposium, San Diego, CA, Page 1-14.
4. Munir, K., and Mohammed, L. A. (2019). Comparing user authentication techniques for fog computing. In *Advancing Consumer-Centric Fog Computing Architectures* (pp. 111-125). IGI Global.
5. He D., Gao Y., Chan S., Chen C., Bu J. (2010) An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc Sensor Wireless Network 10(4): Page 361-371.
6. Fernández-Otoya, F. A., Raposo-Rivas, M., and Halabi-Echeverry, A. X. (2022). A qualitative systematic literature review on phonological awareness in preschoolers supported by information and communication technologies. *Education Sciences*, *12*(6), 382.
7. Jansen W, (2003) "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium
8. Pradhan, S., and Giri, C. K. (2016). Role of different cryptographic algorithms in information security on web. *International Journal of Engineering and Management Research (IJEMR)*, *6*(5), 339-345.
9. Ever, Y. K. (2018). Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. *IEEE systems journal*, *13*(1), 456-467.
10. Bokolo, A., Maureen, G. P., and Majid, M. A. (2021). A web deployed multi-agent based approach for student-lecturer appointment scheduling in institutions of higher learning. In *Journal of Physics: Conference Series* (Vol. 1830, No. 1, p. 012007). IOP Publishing.