Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 5, May 2022, pg.40 – 50

An Enhanced Security Model for Simple Reformation-Based Password Scheme using PHP

Ms. Poonkodi R[1]; Jawahar Sriraam S R[2]; Deepakvel M[3]; Gokulnath J[4]; Jagathishprabu S[5]
[1,2,3,4,5]Department of Computer Science and Engineering, Sri Eshwar College of Engineering
[1] poonkodi.r@gmail.com; [2] jawaharsriraamsr@gmail.com; [3] deepakvel3@gmail.com;
[4] gokulnath11405@gmail.com; [5] jagathishprabu@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i05.004

Abstract*-- Lack of security has become a major concern, given the prevalence of attackers, hackers, crackers, scammers and spammers. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access a given system or resource. Existing authentication processes are usually accomplished by user ID and password, with the authentication schemes Pair-based Authentication scheme based. Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this research paper, two different techniques are proposed to generate session passwords using text and colors which are resistant and more secured. These methods are suitable for Personal Digital Assistants. These methods are suitable for Personal Digital Assistants. This scheme can authenticate the user by session passwords that are used only once. It is no longer useful if the session is terminated. For every login process, users have to feed the input with different passwords. It provides better security against dictionary and brute force attacks as password changes for every session. The proposed authentication schemes use text, colors and images for generating session passwords.

Keywords: Security; Authentication techniques; data attacks; password scheme; colour password session.

I. Introduction

Passwords are the most general form of user authentication technique used in various computing applications like banking ATM, websites, operating systems login and mobile phones. However, user's passwords are cracked and bargained under different vulnerabilities. There are different types of password attacks and describes the authentication techniques by justifying the resistance to existing password attacks. Finally, it presents a password based secure authentication mechanism to resist some password attacks in different computing applications. Shoulder surfing is one of the password attacks in which the adversary detectives the user's movements to steal their passwords. Eventually, the attackers can observe and use all the options related to the password length. The brute force attacks pattern all possible combination of password until the correct one is received to break the authentication method It is a time consuming as searching all combinations and mostly used to crack the encrypted passwords. It is effective for small length passwords. The dictionary attack is a form of brute force attack but faster the brute force attack and it attempts to match the password with mostly used words in our daily life. In this technique, the attacker creates the dictionary of most commonly used words and they can use these words to break the authentication mechanism. Another password attack is Key Loggers which are software programs installed in user computer and monitors the user activities by copying the key pressing activities of user. The attackers crack the authentication technique using the log file which stores all the history of key pressing activities and the log file will be forwarded to the attacker's e-mail. A web-based password attack is called phishing in which the attackers redirect the user to the fake website whose interface is like real website to attract the user to crack the password by retrieving the login information from the fake website. Replay attacks is also called as reflection attacks which focused on the user authentication method. In this attack, the attacker initially enters his/her password first time login phase. The receiving device sends the trial to the sender to authenticate the method. The attacker utilizes the process and responses of the receiving device which can able to accept the challenges of the attacker. The standard process of password scheme allows the users to log into the system by his/her username and password then the system validates the user by matching the user database and grant the access. Although, the benefit of this scheme is to provide the security of data by handling only the authenticated users, this schema is vulnerable to password attacks such as shoulder surfing, key loggers, phishing and brute force. If security breach happened in the authentication system, the valuable and private data confidentiality will

become vulnerable. In some cases, it may cause to unauthorized access to the data and the hardware resources, loss of wealth, privacy issues. For example, our g-mail, google drive accounts, google contacts, hangout chats are handled by a single google account. More than that our android smartphones also integrated with the google account. If any attacker got access into our google account, it will be a catastrophic damage for our data and the privacy. In this paper we are proposing a secure password authentication mechanism and authentication technique and it resists shoulder surfing, brute force and key logging attacks in any computing applications.

II. Related Study

In this section, we review and analyze the recent studies of panel-based authentication techniques proposed by researchers in the literature.

2.1 Authentication method

It works with 8*6 matrix or grid which consists entire 26 English alphabets in capital, 10 numerals and 12 chosen symbols. The characters are organized in the matrix in random manner. In the authentication process the user will enter the position (row number followed by column number) of each character in the password and for last three characters he will enter the same characters which is in the password. In the Figure 1, sample matrix if the password is ' 1DEI*2DTA#3' then the user needs to enter as '6463131582226316A#3'.

2.2 Pair based scheme

By 6*6 matrix which is filled with 26 capital English alphabets and 10 numerals. In the authentication process the user take the characters of the passwords as pairs. The row will be selected from the first letter of the pair and the column will be selected by the second letter of the pair. The intersection point of the row and column will be taken as the part of the session password. After this the distribution of the characters in the matrix will be change for the next pair.

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

Fig. 1. Pair based scheme

2.3 Graphical Password Schemes

In graphical password authentication system was designed to protect the users against weak as well as strong shoulder surfing attacks. The proposed system uses a database of different icons, where the user selects a few icons as a password. The user also selects a ball of specific color out of five balls of different colors. The chosen color ball is used to authenticate a password icon as and when the ball moves over the icon. Although the system resists against both weak and strong shoulder surfing attacks, it takes high time cost during the authentication process, and the user has to wait for a dynamic moving ball to coincide over his/her required password icon so that the user confirms his/her password icon by pressing the space key or any other key of the keyboard. It shows that the scheme is not suitable for a real-time system. A graphical-based textual password scheme was introduced. For each password character entry, the user has to click inside the area of an imaginary triangle made up of three vertices of the user's password characters. The scheme is resilient to shoulder surfing attacks, but the login process is lengthy, complicated, and difficult for successful login entry. The scheme is not suitable when the user has to enter the password frequently after every short interval, as in a mobile phone.

2.4 Brute Force Algorithms

In brute force algorithm, searching a string pattern was initialized which was an excellent attempt to search for a pattern efficiently by ignoring the middle section of the string, but it will give a better result if the pattern length is more significant than four characters. The algorithm will compare the first and last characters for four characters, but the time saved against the rest of the two characters is less than the time consumed for multiple if-else statements. Moreover, if the first and last character matched for a long string, the rest does not need to match. Instead, they will require further comparison for the rest of the characters. Suppose any mismatch occurred in the central characters. In that case, the substring will be ignored, and the algorithm will move onward, e.g., the first and last characters of the strings introduced and interested are matched, but the central characters mismatch.

III. Proposed Methodology

The proposed research work is implemented with enhanced authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration. The proposed implementation was done using PHP platform and MySQL database management system.

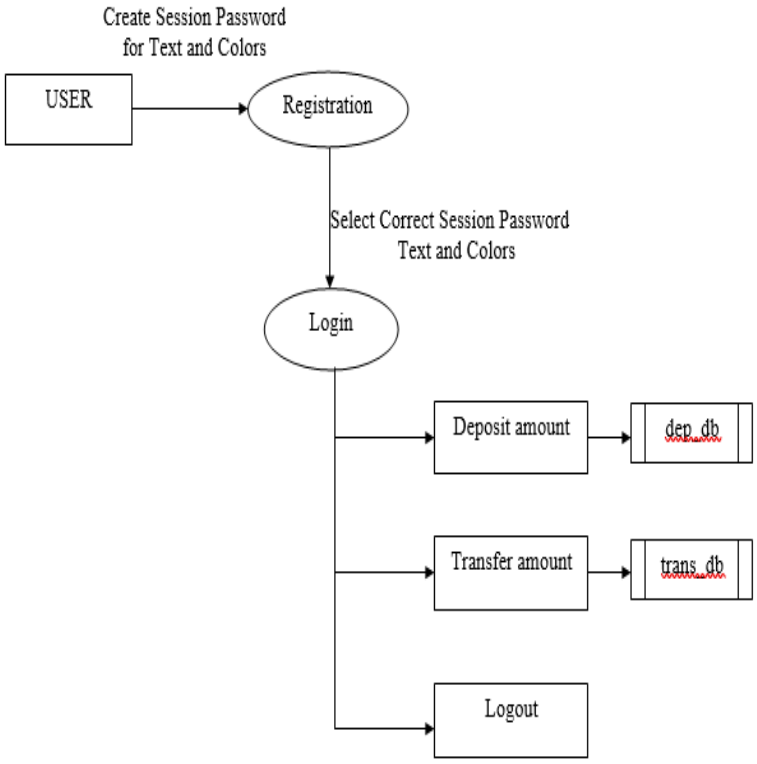

Fig.2. Data flow diagram

Figure 1 describes about the entire process of proposed research model as; a user can create a session password for the text and colors for new registration. Now, the existing users can login into the system using correct session password text and colors for successful and secure entry. Once the login of user completed successfully, the proposed model can take the users to perform the process such as deposit amount and transfer the amount. After the process completed user can logout from the model.

The below mentioned figure 2 designed for user registration and login model for proposed concept using MYSQL database with different key such as foreign key and primary key. The color and text passwords are created for each account to manage the different user's login.

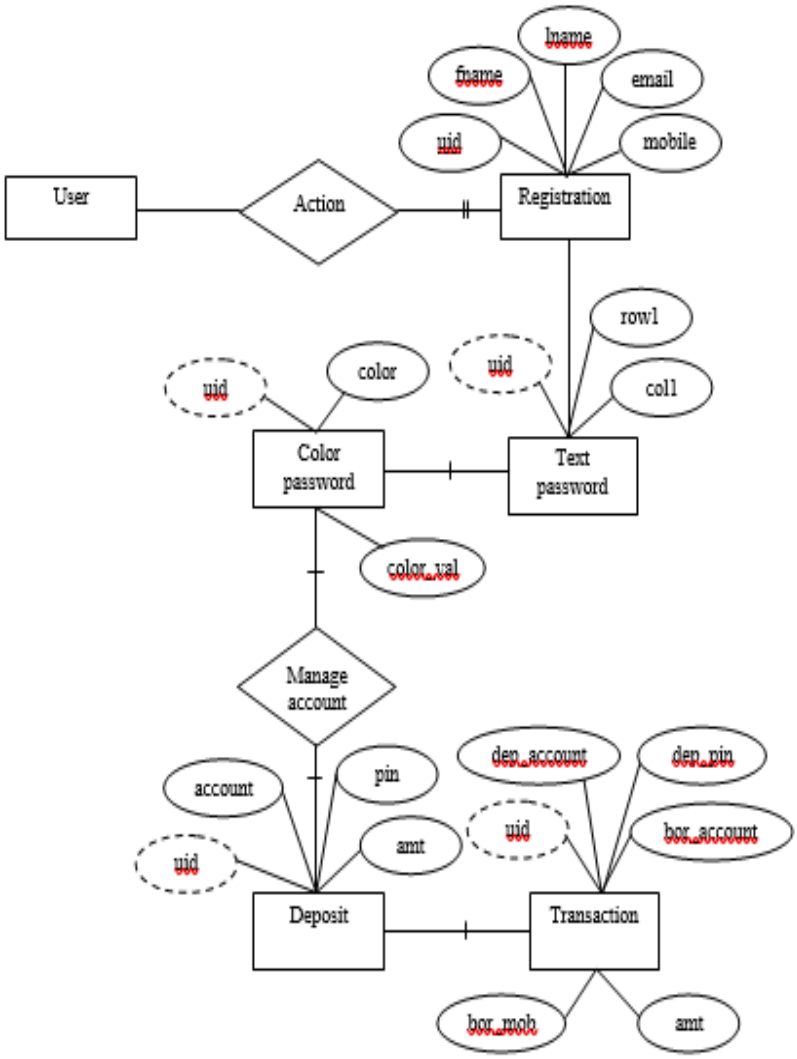

Fig. 3. ER diagram

IV. Result & Discussion

The proposed implementation is explained in detail about creation of successful user login and processing the transaction of financial needs in a secured manner. The below figure 4 explained about the registration of new user login with their personal details as input data for account creation. After feeding the mandatory and correct details of user registration of user will be created for login into the proposed system in two way secured models as text and color matched password system.

Fig.4 User registration page

The proposed system designed with three stages like account creation, login and transaction of money. In the figure 4, the registration page requested to fill some mandatory information about the user for creating the secured login with enhanced security method.

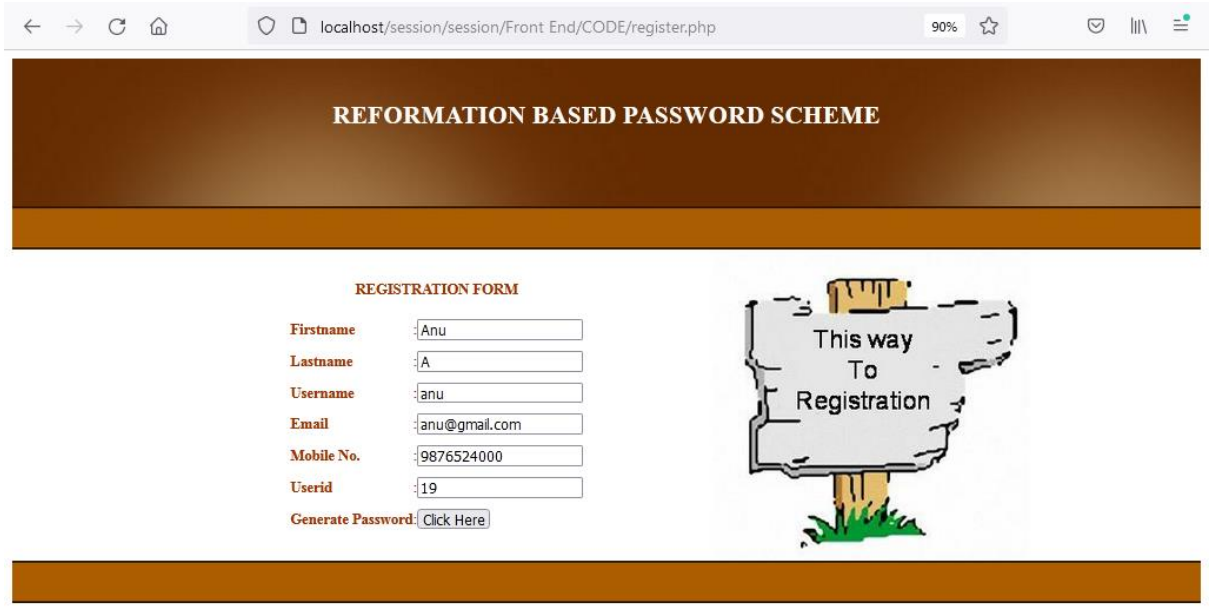

Fig. 5 User feed their data to create successful login

There are some parameters such as first name, last name, username, mail id, contact number and user id for uniqueness. After the successful feed of user data, the option named generate password is provided to create a unique password for each and every user by their own are explained in figure 5.

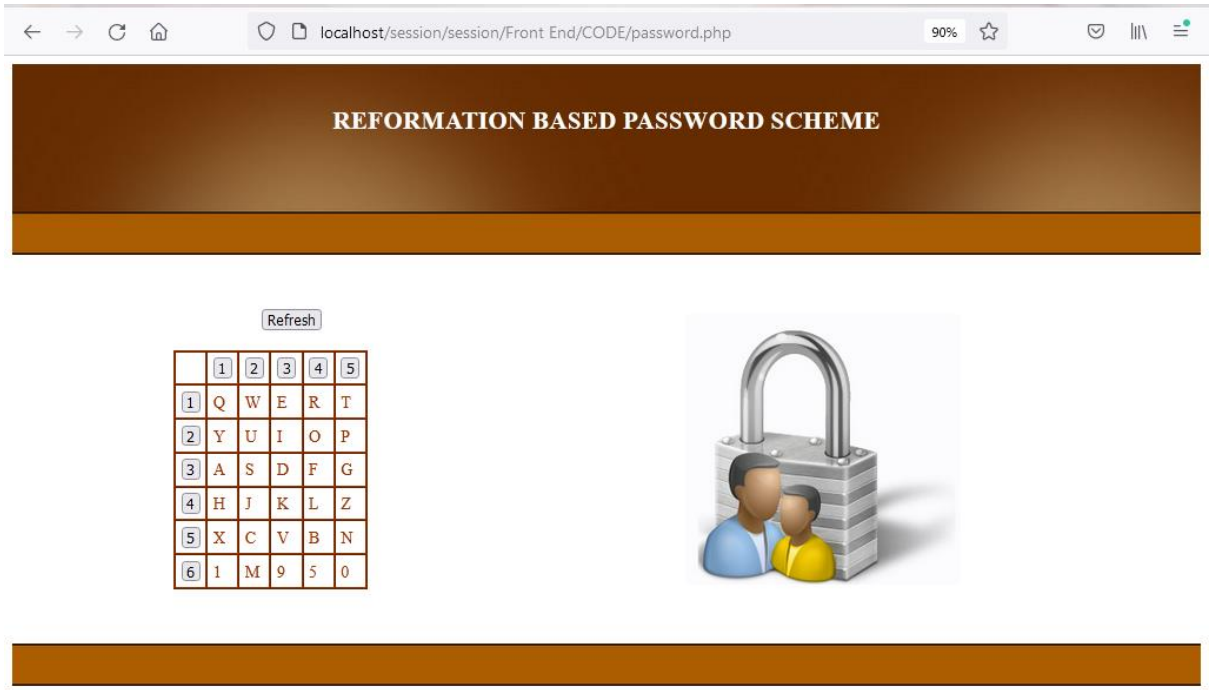

Fig. 6 Password text-based system

In figure 6, the text- based password system is generated for each user based on their input data and parameters selected is explained.

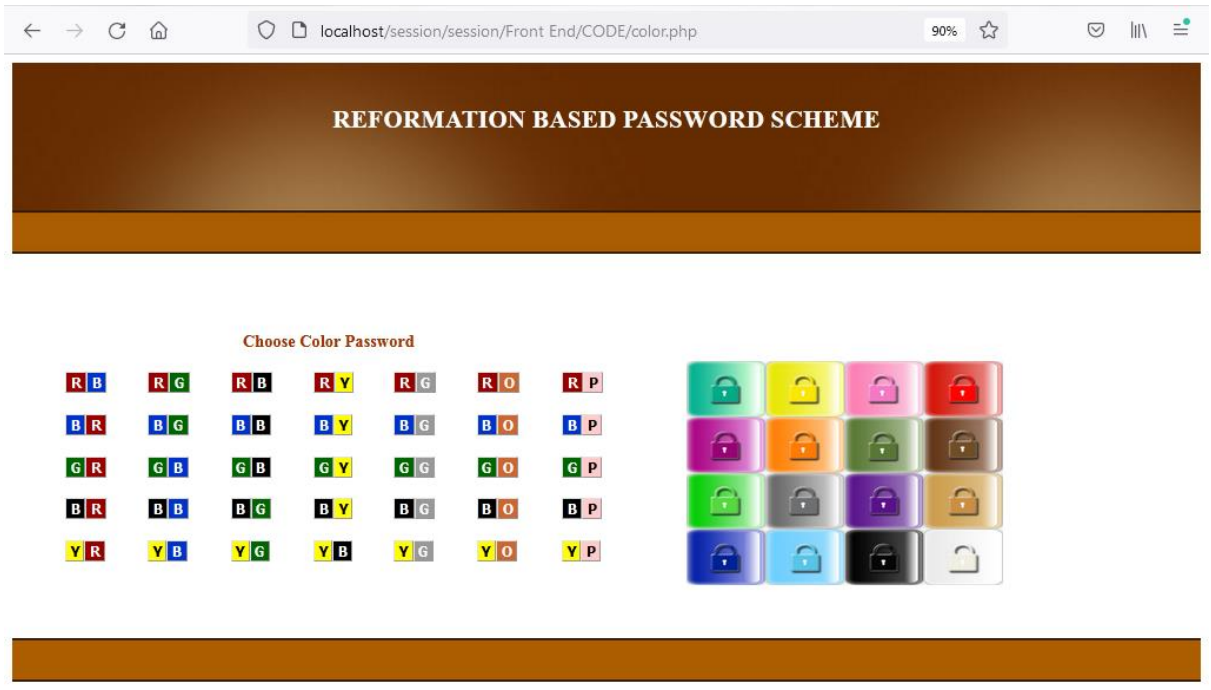

Fig. 7 Password color-based system

In figure 7, the color- based password system is generated for each user based on their input data and parameters selected with color password scheme which is enhanced with high security model.

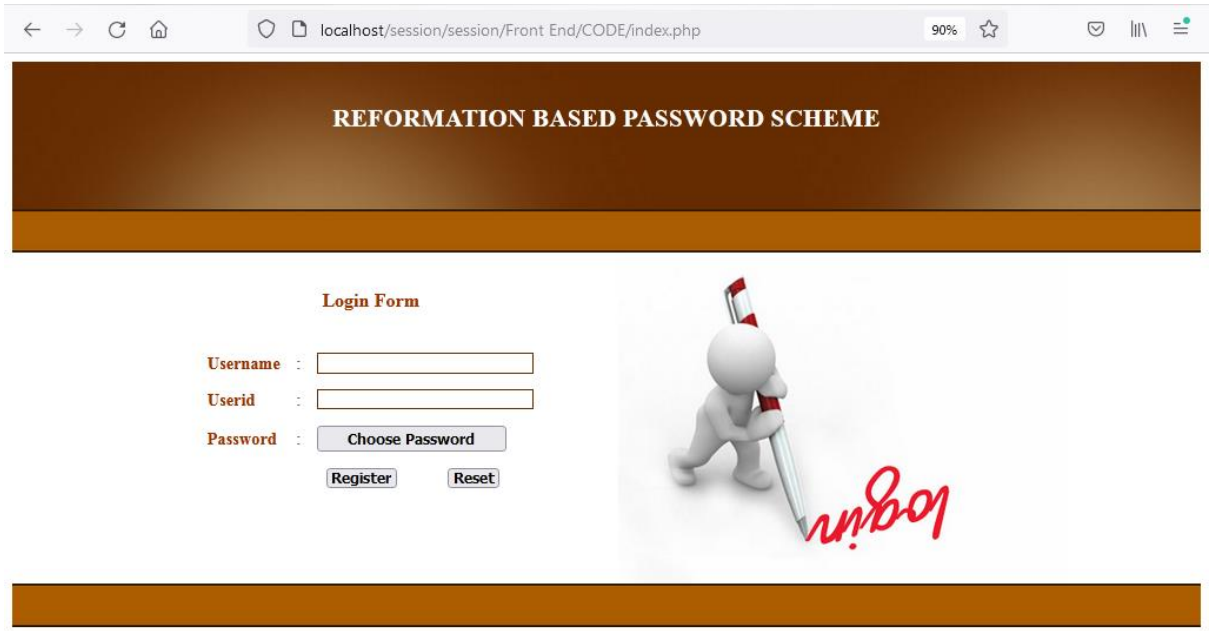

Fig. 8 Login page after successful account creation

In figure 8, after the creation of successful login of the user with two-way enhanced security system as text- based password and color- based password is generated. After the creation of login with uniqueness, the proposed model prompt for user login with two different passwords.

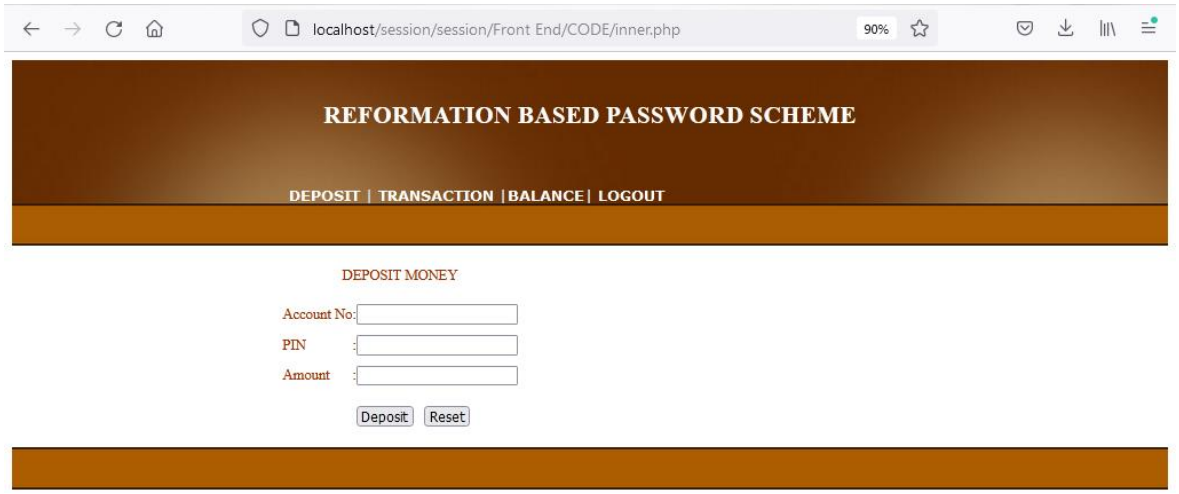

Fig. 9 Home page to deposit money

Figure 9 is explained about the transaction of money from the user account with reformation-based password scheme. The user account details with how much money user would like to deposit with other end user will be done using their registered user pin for successful transaction of the amount in a secured way. After the successful completion of the transactions the user can check for their available balance in his/ her account. The proposed system will be processed with reformation- based password system which was more secured with two enhanced security model to protect the user information from the third- party access of the data.

V. Conclusion

The application works according to the restrictions provided in their respective browsers. The application satisfies the Admin. The speed of the transactions become more enough with enhanced security model and the proposed system helps the user to create their own login based on the two proposed unique schema for secure login and it helps to protect the data more protective method.

The text and color password are the two different password are implemented for enhancing the security protocol and the research has been successfully developed and interpreted and system was developed according to the admin requirements. The system produces accurate results and it also reduces a lot of overheads, which the manual system faced. The information requirements may still increase. As future enhancement, it is essential to change the software when new software arrives with more advanced feathers. So, it is much necessary for further development.

References

[1]. Savita, et.al., "A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 11, November 2015.

[2]. Silva, et.al., "Authentication and the Internet of Things", ICSEA: The Twelfth International Conference on Software Engineering Advances, 2017.

[3]. Rahul M & team, "Prevent shoulder surfing using graphical and duo letter authentication", IJARIIE-ISSN (O)-2395-4396, Vol-2 Issue-2 2016.

[4]. S. Subangan and V. Senthooran, ``Secure authentication mechanism for resistance to password attacks," in Proceedings 19th International Conference Advance ICT Emerging Regions (ICTer), vol. 250, pp. 1-7, 2019.

[5]. M. Zubaidie and J. Zhang, ``RAMHU: A new robust lightweight scheme for mutual user authentication in healthcare applications," Secure Communication Network, vol. 20, pp. 1-26, Mar. 2019.

[6]. H. Channabasava and S. Kanthimathi, ``Dynamic Password Protocol for User Authentication," in Proceedings Intelligent Computer Conference, Switzerland: Springer, pp. 597-611, 2019.

[7]. W. Luo, et.al., ``Authentication by encrypted negative password," IEEE Trans. Inf. Forensics Security, vol. 14, no. 1, pp. 114-128, Jan. 2019.

[8]. E. Erden, ``One time password as a service,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 3, pp. 743-756, Aug. 2018.

[9]. S. Zaman and M. Zalisham, ``A text-based authentication scheme for improving security of textual passwords,'' International Journal of Advance Computational Science & Applications, vol. 8, no. 7, pp. 513-521, 2017.

[10]. S. Umar, and M. H. Khan, ``Secure pattern-key based password authentication scheme,'' in Proc. Int. Conf. Multimedia, Signal Process. Commun. Technol. (IMPACT), pp. 171-174, Nov. 2017.

[11]. Gokhale and V. S. Waghmare, ``The shoulder surfing resistant graphical password authentication technique,'' Procedia Comput. Sci., vol. 79, pp. 490-498, Dec. 2016.

[12]. J. D. Still and J. Bell, ``Incognito: Shoulder-surng resistant selection method,'' Journal of Information Security Appl., vol. 40, pp. 1-8, Jun. 2018.

[13]. Disabled People in the World in 2019: Facts and Figures. Accessed: Nov. 19, 2020. [Online]. Available: https://www.inclusivecitymaker.com/disabled-people-in-the-world-in-2019-facts-and figures.

[14]. Z. Yun, and X. Han, ``Alpha pwd: A password generation strategy based on mnemonic shape,'' IEEE Access, vol. 7, pp. 119052-119059, 2019.

[15]. S. Kanhere and team, ``Recent trends in user authentication: A survey,'' IEEE Access, vol. 7, pp. 112505-112519, 2019.

[16]. H. Yang, ``A mobile authentication system resists to shoulder-surfing attacks'', Multimedia Tools Appl., vol. 75, no. 22, pp. 14075-14087, Nov. 2016.

[17]. C.-Y.Wang, ``Shoulder-surng-proof graphical password authentication scheme,'' Int. J. Inf. Secur., vol. 13, no. 3, pp. 245-254, Jun. 2014.

[18]. R. Akbar, and R. Aamir, ``Authentication model based on reformation mapping method,'' in Proc. Int. Conf. Inf. Emerging Technology, pp. 1-6, Jun. 2010.

[19]. M. Shakir and A. A. Khan, ``S3TFPAS: Scalable shoulder surng resistant textual-formula base password authentication system,'' in Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol., pp. 12-14, Jul. 2010.

[20]. Van Oorschot, ``A research agenda acknowledging the persistence of passwords,'' IEEE Secur. Privacy Mag., vol. 10, no. 1, pp. 28-36, Jan. 2012.

