An Authentication for digital transaction with OTP using Color Code Systems (CCS)

Shivamurthaiah M[1] Sitesh Kumar Sinha[2], Praveen Kumar K[3] Manasa L R[4]

[1*]Dept. Computer Science and Engineering, AISECT University, Bhopal, India
[2] Dept. Computer Science and Engineering, AISECT University, Bhopal, India
[3] Dept. Computer Science and Engineering, AISECT University, Bhopal, India
[4]Department of Computer Science, Davangere University, Davangere, India

Corresponding Author: shivamurthaiah@gmail.com   Tel.: +91-9538114756

Abstract— An Authentication for the digital transaction is a most vital problem. To secure any transactions through digital, mobile, internet, online system is very important. Nowadays India is gradually moving towards digital transactions. To make sure the confidential transactions are very important. The textual password for the Authentication is the most common method, here user need to memorize their passwords during their transaction, somewhere it is vulnerable to social engineering, cyber-attacks, and shoulder surfing. Regarding this, some graphical passwords are introduced to avoid the textual passwords. To address this problem, we can implement an application called color code system with OTP. It is a new technique based on the graphical password, in which here we use an OTP and color coding to solve the security problem. Here once the colors are exhibited with a specific rating, after this, some passwords are generated with some evaluation of colors, further the same colors are brought forth in a random path., we can insert the passwords according to the previous colors and ratings for user authentication which is called color code authentication, by this technique we can overcome the attacks like shoulder surfing.

Keywords— Authentication, Transaction, Color, Ratings, Shoulder Surfing

I. INTRODUCTION

Nowadays, online banking is a common method to transact our banking, it is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transaction through the financial institutions' websites. Online banking is also known as internet banking, e-banking or virtual banking. Transfer of funds by using electronic devices. Online banking helps the less use of paper, i.e., Paperless banking. The online banking process is very user-friendly and fast, as compared to the core banking system. Moreover, the transaction of account with security is a very big issue, regarding this authentication of bank transaction, is carried out through some of the textual passwords, somewhere it is vulnerable to shoulder surfing, randomly we use lengthy passwords to secure our transactions. But here the main problem is the hardest to memorize the passwords suppose we use a short password that is easy to memorize, such words can be easily guessed or broken up by the shoulder surfing to avoiding these we proposed a system called CCS [Color Code System] in which here we are using different colors with number of ratings for authentication.

There are many alternative techniques like graphical passwords and biometrics, such as fingerprints, iris scan or facial recognition has been introduced [1]. But these from the system too costly and not easy to take. The primary disadvantage of this overture is that such system can be expensive and the recognition process can be tedious. On the other hand, there are many graphical password schemes like color, images and grayscale images that are nominated in the last decade [2], which are resistant to and other problems like usability issues and using up so much time for user transaction. Only most of them facing shoulder surfing attacks, which is quite the vital problem, regarding this our paper represents a technique CCS [3].

Present System of online Transaction Security:

Security of a customer's money info is incredibly necessary, knowing   these money establishments have created numerous security processes to   cut   back   the   chance of unauthorized on-line access   to   a client record.   The secured web site for the aim of transactions is universally accepted.   Banks guarantee web banking   security for patrons by exploitation coding technology like secure sockets layer   –verifying web banking   account   activity, although single secret authentication is in use, there ar some countries suppose that on-line transactions aren't   secure

enough. Here we are able to contemplate some totally different security ways in use for on-line dealings. The PIN/TANs wherever the pin represents a secret, used for the login and TANs representing one-time passwords to demonstrate the dealings. There ar many ways to send Tans, therein the popular one is to send an inventory of tans to the web banking user by communication letter. In our own way of exploitation tans is to get them by would like employing a security token. These token generated tans depend upon the time and a novel secret, keep within the security token (two-factor authentication or 2FA [4]).

II. METHODOLOGY

Many options of web banking are positive; however, some negative prospects additionally exist within the digital world that would keep a lot of cautions customers away. For avoiding this, during this paper we've got projected authentication system for bank dealings with some OTP with color codes, OTP is nothing however a one-time secret the foremost necessary advantage that's self-addressed by OTPs is that, in distinction to static passwords, they're not prone to replay attacks together with this we tend to use color grids, initial we tend to use a colors with some ratings that are known as code scheme[5], that we tend to will use in our application, once user may be projected to dealings it may be generated initial, when this the similar range of OTP is generated, throughout getting into the OTP there's possibility somebody understand our OTP and it's going to be an opportunity to knowing or stealing of our dealings info for avoiding this we tend to use range of OTPs. This authentication system known as code authentication with OTP.

NEW AUTHENTICATION SCHEME

In our project we proposed a system password which is known as "Color code authentication with OTP" to authenticate our digital transaction, here we can use some color grids with some ratings [6, 7, 8, 9]. When user wants to transact with his account, first some number of color grids will be displayed with some ratings all the color grids have to contain separate ratings, in this phase user must know the ratings of the specific color grids, after this separate OTPs will be generated with respect to the colors and ratings, user must enter the OTP according to the ratings, OTP which can shows one-time password[10,11,12], in which, the OTP generation can generate only one password, in this proposed paper we are going represent number of OTPs with similar number of color and ratings, this is what we called second layer of authentication. Suppose color grids are in RGB assuming the ratings are 123 and the passwords are ABC if the RGB color grids are in random order GBR user must

enter BAC in this way we can give a security to our transaction or we can say encrypted color grids.
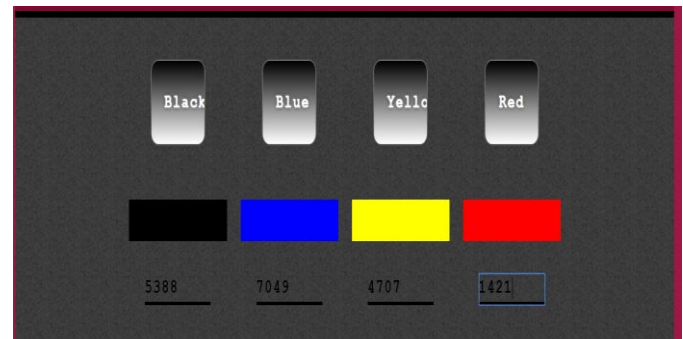
III.   DIAGRAM AND FLOWCHART
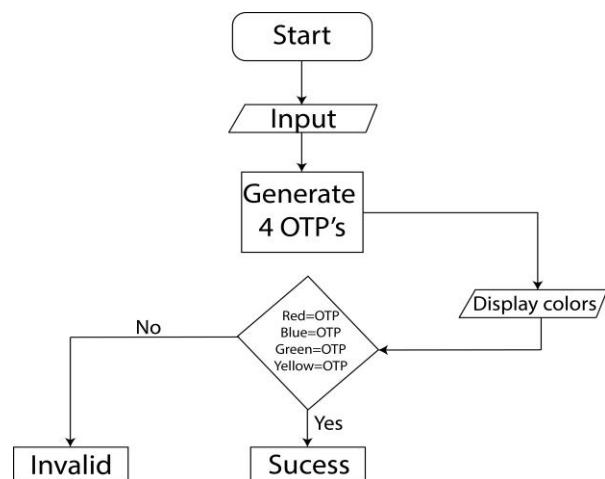

Figure 1 Color Code System

A.   Abbreviations and Acronyms

Color Code System – CCS

One Time Password – OTP

Personal Identification Number- PIN

Transaction Authentication Number – TAN

IV. CONCLUSION

In this paper, we proposed authentication techniques based on colors with OTPs. These techniques generate a number of OTPs. The techniques use colors grid for generation of OTPs. Pair based technique requires no special type of registration, during digital transaction, color grids will be generated after this. The grid displayed a similar number of OTPs. Ratings should be given to colors, based on these ratings and the grid displayed during the transaction, the similar number of OTPs are generated and the user must enter these passwords according to the colors and ratings. However, these schemes are completely new to the users and

the proposed authentication techniques should be verified extensively for usability and effectiveness.

ACKNOWLEDGMENT

REFERENCES

[1]. X. Suo, Y. Zhu and G. Owen, "*Graphical Passwords: A Survey*". In Proc. ACSAC'05. Vol5 Feb 2015, 2277128x

[2]. G. E. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.

[3]. Rami El Sawda, & Habib Hamam *RGB Coloured Image Encryption Processes Using Several Colored Keys* Images"

[4]. A. F. Syukri, E. Okamoto, and M. Mambo, *"A User Identification System Using Signature Written with Mouse*," in Third Australasian Conference on Information Security and Privacy (ACISP), pp. 403-441.

[5]. M Sreelatha , M Sshashi , M Anirudh , MD Sulthan Ahamer, V Manoj Kumar ."*Authentication Schemes for Session Passwords using Color and Images*",International Journal of Network Security &Its Applications, Vol.3,No.3,May 2011.

[6]. *Nirmala.B, Manigandan.T, Kumanan.K."Authentication Schemes For Session PasswordsUsing Text And Colors",IJEDR, Vol5, Issue 2, 2017.*

[7]. Z.Zheng, X.Liu, L.Yin, Z.Liu "*A hybrid password authentication scheme based on color and text*" Journal of computers-May 2010.

[8]. S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "*Authentication Techniques For Engendering Session Passwords With Colors And Text*" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[9]. Rohit Jagtap, Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher "*Authentication schemes for session password using color and special characters*" International Journal of Innovations & Advancement in Computer Science, April 2014.

[10]. Rachita Dubey, Jijo S.Nair, "*A Review on Secured One Time Password (OTP) Based Authentication & Validation System*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.6, pp.232-236, 2017.

[11]. Salim Istyaq, Lovish Agrawal , "*A New Technique For User Authentication Using Numeric One Time Password Scheme*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.5, pp.163-165, 2016.

[12]. Dr.D.S. Rao et. al. ," *One Time Password",* Securty Journal of Computer Technology and Applications, Sept-Oct 2011. Vol(2)5, ISSN:2229-6093

Authors Profile

Shivamurthaiah M pursed Masters in Computer Science from Kuvempu University of Karnataka, India, in 2006 and Master of Technology from KSO University in year 2013. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science, Garden City University,Bengaluru. He has published 14 research papers in reputed international journals. main research work focuses on Cryptography Algorithms, Network Security, Image Processing and Software Engineering Data Mining, IoT and Computational Intelligence based education. He has 10 years of teaching experience and 4 years of Research Experience.

Sitesh Kumar Sinha ,He currently working as Pro V C AISECT University. He has published more than 28 research papers in reputed international journals. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has more than 18 years of experience in both acadmic and academic administration.

Praveen Kumar K pursed Masters in Computer Science from Karnatak University of Karnataka, India, in 2006 and Master of Technology from KSO University in year 2013. He is currently pursuing Ph.D. and currently working as Lecturer in Department of Computer Science, CFC, Davangere. He has published 4 research papers in reputed international journals.

Manasa L R pursed Masters in Computer Science from Davangere University of Karnataka, India, in the year 2017.