ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

COLOR CODE AUTHENTICATION ATM TRANSACTION FOR ENHANCE SECURITY

Ms Dumbre T.M.*[1], Ms.Priyanka Dherange[2],Ms. Ankita Bangar[3] & Ms. Nikita Auti[3].
Information Technology, Jaihind Polytechnic, Kuran
Pune India

ABSTRACT

We present a system that gives higher security for ATM transactions. In this system, the color code technique is used. Here, when user's login takes place successfully he/she is directed to Color Code authentication page. Where the user enters his/her favorite 3 colors in the form of color code generated by system to authenticate whether user is valid or not. If valid then user is redirected to Transaction page where user can carry out his/her own ATM transactions else he/she is directed to login page. In this way by applying the technique of Color Code we are enhancing the security of login for ATM Transactions, as the attacker don't know the users favorite colors and even if he/she (attacker) does know those colors, it is not possible to unveil the color code combination which is generated dynamically in our system for carrying out final Authentication process as that color code is encrypted and then sent to user's personal contact number.

***Keywords**:* Cloud, CSP, Denial, IS, Cloud Security,Cloud Service Availability.

I. INTRODUCTION

Authentication verifies the identity of an Account Holder. Authentication is important for providing Security of the System. Authentication is done by String of alphanumeric and Special Characters that allows access to the computer, interface... etc. and also called password. Password is the Key to authenticate user account. Text key (password) is the most common method for authentication. The general method is more vulnerable to various cyber-attacks like phishing, spyware attacks, dictionary attacks, brute force attack etc. To overcome the problems faced by general method alternative authentication models like biometrics used. But the biometric authentication is for Top level security and this authentication system involves a lot of expense. Now a days there more talked about graphical password in the industries. Now a day's banks and financial institution using one time password and it was also called as OTP. Besides OTP offers better security. it is impossible for hacker to break into the OTP Using conventional attack. But the OTP was very expensive it is not for general purpose user, we introducing new kind password matrix which solves most of the problems like phishing, spyware attacks, dictionary attacks, brute force attack. The color code matrix password was only used for the only one time like OTP because it changes for every refresh of the page. The color code matrix password is virtual password it was created by system for that instinct.

The color code matrix password contains alphabets and numeric values which was represented in six rows and six columns. It was arranged in 6*6 matrix or grid. The each row [0] and column [0] contains the color background. The color includes anyone in the set, the colors in the set are red, yellow, green blue, white, and pink. The background color was chosen randomly. The background color varies for each refresh. With the use of color code matrix you can openly type your password the people around you cannot know your password, the color code password matrix cannot be detected or guessed by any software, the color code matrix overcomes the fear of brute force attack, dictionary attack.

ISSN 2348 – 8034
Impact Factor- 4.022

II. METHOD & MATERIAL

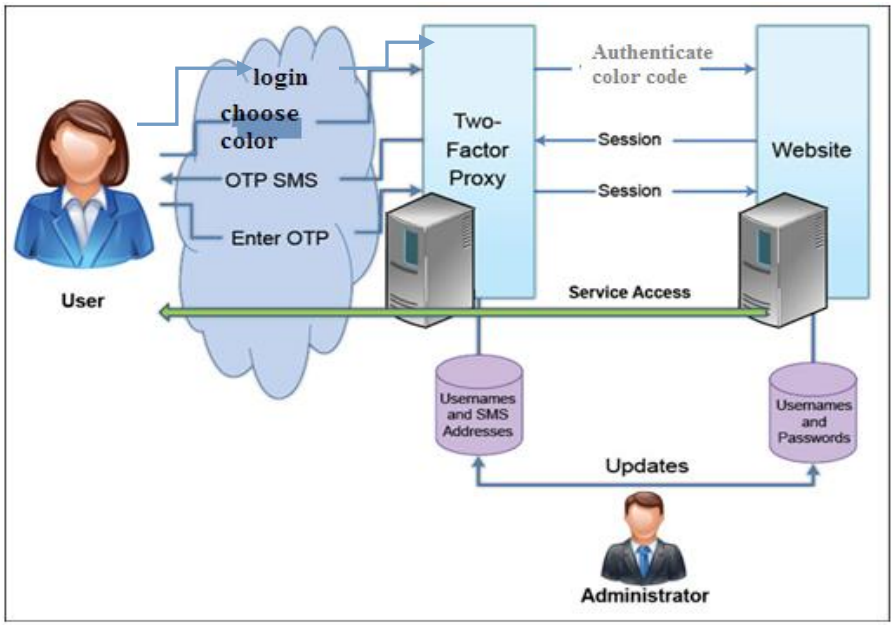

Fig1.Architecture of color based ATM System

1. Color coded encryption

Converted in ASCII value ASCII is the abbreviation of American standard code for information interchange it typically based on English, the character are converted into ASCII value

2. Grouping the ascii value

The converted ASCII values are grouped in four digits, if the character is sort of four digits zeros are added to the last part

3. Assigning The Color Code

The each grouped part contains four digit numbers these numbers represent the html color codes, the each part is assigned respective color codes.

4. Converted Into Binary Values

After assigning the color codes the each color code is converted into binary values.

5. Comprassion Of Data

The converted binary values are too large for transmitting or storing to reduce the size we use XOR to reduce the size of the data

Feasibility study

- To enhance security for ATM based transactions.
- To reduce fraud during ATM transactions.
- To check ATM Security

ISSN 2348 – 8034
Impact Factor- 4.022

III. OTHER SECTIONS

The concept of using RGB color code encryption is an innovative idea, The RGB color model is combinational of three different types of color. The combinations of red, green and blue light provides huge combination and wider variety of color spectrum. The general uses of the RGB color model is to project the images in electronic systems, like movies and photos in television screens and computer monitors and it's also used in high definition photography. CRT, LCD, plasma and LED TV and monitors all uses the RGB model. We are using the similar technique in our project, the each key in the keyboard hold the ASCII key, the combination of ascii key and present time provides us 8 bit to 24 bit RGB color representation, these 8 to 24 bit representation gives access to 16 million different colors.

Proposed System

1) Module Level 1- Login Panel
2) Module Level 2-Registration
3) Module Level 3-OTP
4) Module Level 4-Choice color

IV. RESULT & DISCUSSION

Methodology/ Planning of work

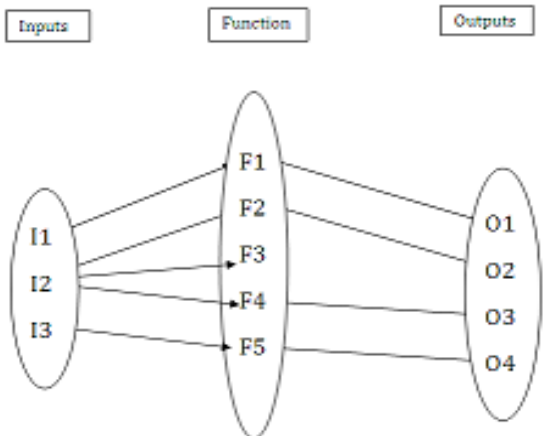

Fig 2.Venn diagram of color code based ATM System

Let S = { I, O, F, Success, Failure}
Where,
I : Set of inputs,
O : Set of outputs,
F : Set of functions,
Success :
Failure :
I ={ I1, I2, I3 },

O = { O1, O2, O3 },
F = { F1, F2, F3, F4, F5 }

Where,

For I –

I1 : Registration form,
I2 : Login form,
I3 : Color code form

For O –

O1 : Registration message (Success or Failure),
O2 : Login message (Success or Failure),
O3 : Color code received (via SMS),
O4 : Color code verified message (Success or Failure).

For F-

F1 : Store information given from registration form in DB.
F2 : Check that valid username and password is entered in login page and display message.
F3 : Generate Color-Code and encrypt it (if success).
F4 : Send Color-code to user through SMS (if success).
F5 : Authenticate Color-Code entered by user and thendisplay message.

Success : Login successful
Failure : Login failed

V. CONCLUSION

Authentication is crucial for computer security. As the color matrix password are attack resistant, there is a growing interest for them. Presently numerous authentication skill and version are available. But, each of them have their own pros and cons. In this paper we have proposed a color matrix password scheme that is more resilient to dictionary attacks, shoulder surfing, spyware and phishing attacks. This 2 step random colored matrix password authentication scheme shows promise as a usable and memorable authentication mechanism.

VI. ACKNOWLEDGEMENTS

First and foremost, we would like to thank my author Ms. DUMBRE T.M., Ms. DHERANGE P.D.,Ms. BANGAR A.A.,Ms. AUTI N.S**.** for his guidance and support. We will forever remain thankful for the constant help and guidance extended by guide, in making this paper. Through our many discussions and ideas. The invaluable discussions we had with her, the penetrating question, has all led to the development of this paper.

REFERENCES

1) *Data Compression - DEBRA A. LELEWER and DANIEL S. HIRSCHBERG Department of Information and Computer Science, University of California, Irvine, California 92717 – ACM Journal*
2) *Lossless Data compression techniques - Klaus Holtz, Eric Holtz, Omni Dimensional Networks , San Francisco , CA 94109 – IEEE Research Paper*
3) *RGB Coloured Image Encryption Processes Using Several Colored Keys Images - By Rami El Sawda (IEEE senior member) & Habib Hamam (IEEE senior Member) – IEEE Research Paper*