Data Security Using Graphical Password and AES Algorithm for E-mail system

[1]Bandawane Reshma B., [2]Gangadhar Mahesh M.,[3]Kumbhar Dnyaneshwar B.,

Student,Computer, GCOEARA, Pune, India
[1]bandawanereshma@gmail.com, [2]gangadharmahesh14@gmail.com, [3]dnyanu76@gmail.com

***Abstract*- The main intention of this project is Data Security using the Text-based Graphical pass-word Schemas using color Combination for E-mail system. It secure users data from shoulder surfing attack. Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords instead of pure graphical passwords. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors for E-mail system. Access to computer systems is most often based on the use of alphanumeric passwords. However, users have interested on graphical password, therefore we have been proposed text based graphical password scheme for E-mail application . With the vast introduction of the wireless world, the exchanged information now is more prone to security attacks than ever. In this paper Encryption and decryption process also done to transfer data through E-mail securely. To make the Authentication between two intended users along with the security, server is used. With the help of server, both sender and receiver will get validated. In this project we have to use the Authentication purpose password Schemas using the Text Based Graphical password for the Login for E-mail system.**

Keywords: Graphical passwords, Data Security, Authentication, Encryption, decryption.

I. INTRODUCTION

Because of increasing threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation.

The main intention of this project is Data Security using the Text Based Graphical pass- word Schemas using color Combination password useful for E-mail system and also implement encryption and decryption for securely transfer information through E-mail system .We have also added QR-code for transferring commercial data like –images, websites link, any product information etc on E-mail system. Basically the Text Based Graphical password is useful for resistant the shoulder surfing attack. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice.

Yet traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit.

II. LITERATURE SURVEY

A. Existing System

In 2002, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate.

In 2006, Wiedenbeck et al. proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. In 2006, Wiedenbeck et al. proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. In 2009, Gao et al. proposed a shoulder sur_ng resistant graphical password scheme, ColorLogin, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of ColorLogin is too high and the password space is too small. In 2012, Rao et al. proposed a textbased shoulder suffering resistant graphical password scheme, PPC. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four prede_ned rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

B. Proposed System

In this section, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors for E-mail application and use AES technique for data security. we secure users data in the E-mail system using encryption and decryption , also we have added QR-code for transferring commercial data through E-mail. The alphabet used in the propose graphical password scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/". The proposed scheme involves two phases, the registration phase and the login phase, which can be described as in the following.

A. Registration phase

The user has to set his textual password K of length L ($8 \leq L \leq 15$) characters, and choose one color as his pass color from 8 colors assigned by the system. The remaining 7 colors not chosen by the user are his decoycolors. And, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user's textual password in the user's entry in the password table, which should be encrypted by the system key.

B. Login phase

The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counterclockwise by clicking the "counterclockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel.

C. E-mail system

After successful login user enter into E-mail system. In which user can perform some basic operations like-send mail, receive mail, view mails in inbox etc. For the purpose of securely transferring data through mail AES Algorithm used for encryption and decryption. In this proposed E-mail system QR-code also added for transferring users commercial data. QR-code provide one more step towards security for commercial data.

III. AIMS AND OBJECTIVE

Main aim of developing this model

1. To resist Shoulder surfing attack.
2. Provide data security in E-mail system.

IV. IMPLEMENTATION

Many software applications are available for Data securing for E-mail system. But we will describe a simple and efficient shoulder suffering resistant graphical password scheme based on texts using colors . The alphabet used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols . and /. The proposed scheme involves two phases, the registration phase and the login phase. An algorithm is proposed here which secures the information while being shared on the network using QR code . Barcodes are used for the obvious reasons. They are acceptable worldwide. Various barcode readers are openly available on the internet and barcodes can be widely scanned.

Implementing flow show in following diagram:-

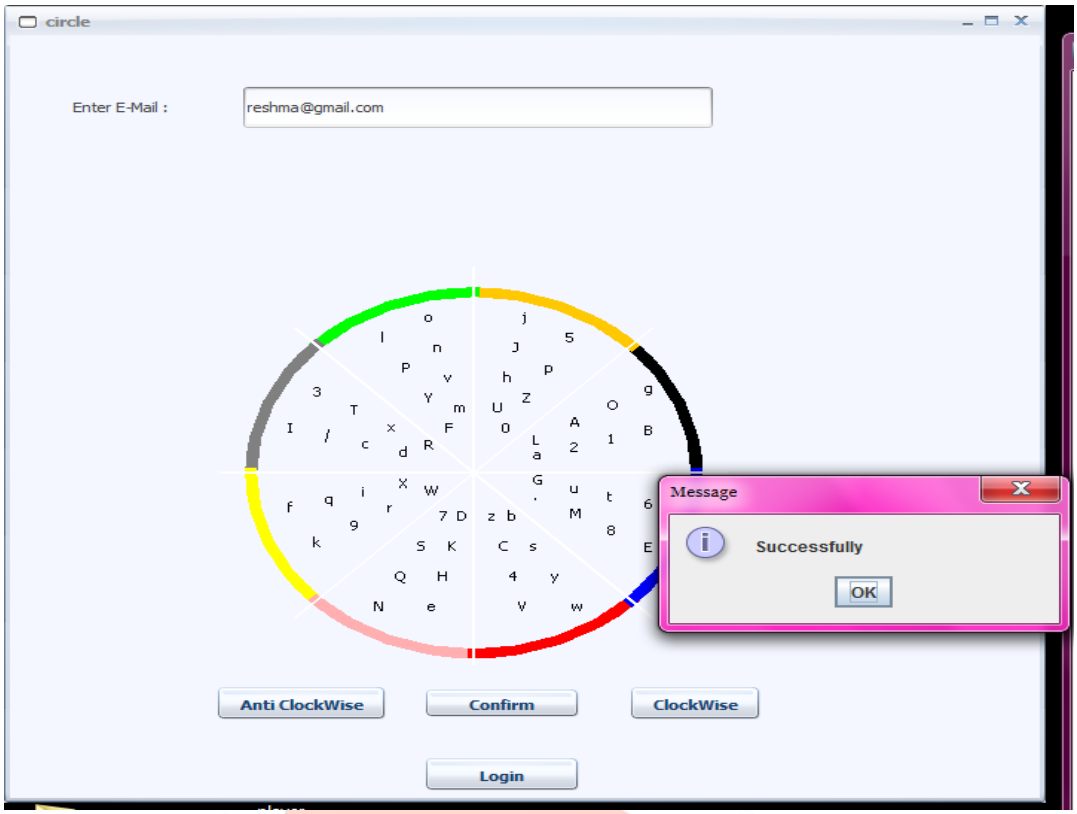

Fig. 1:Graphical Login scheme.

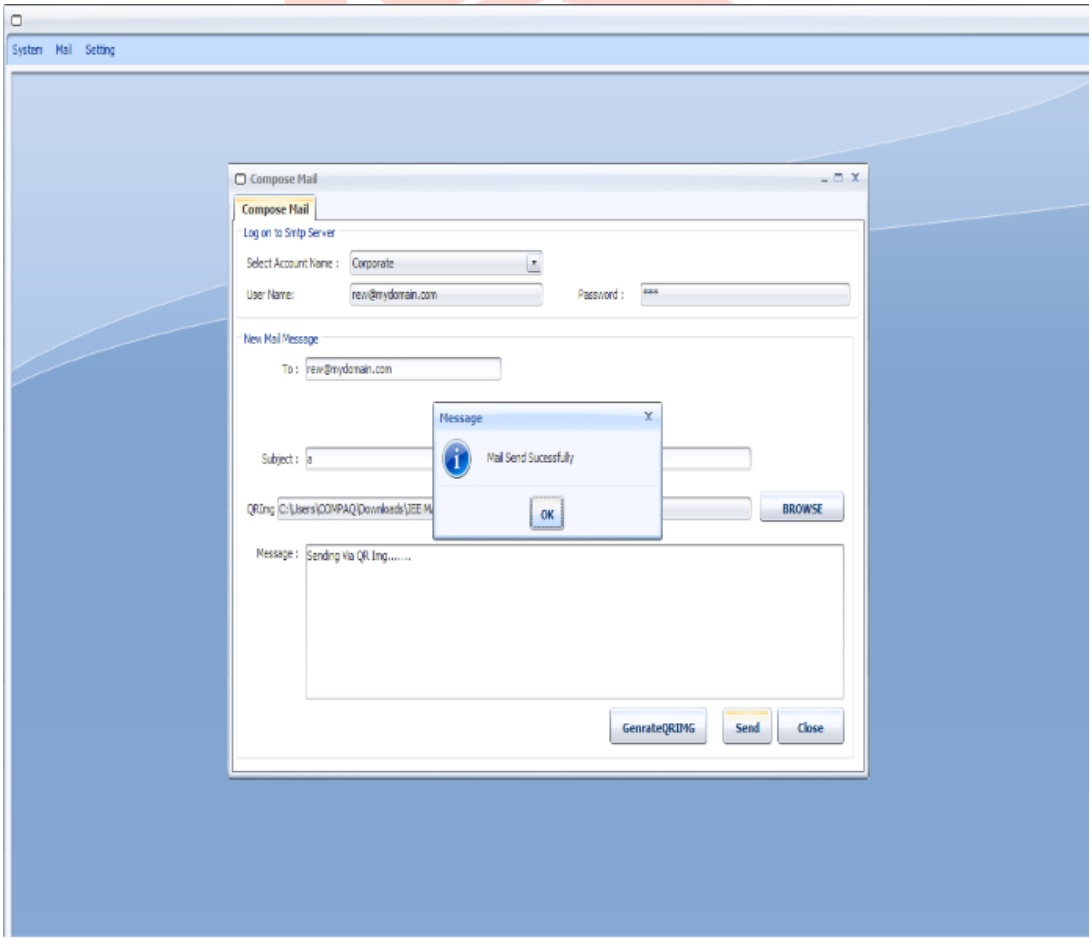

Fig. 2: proposed E-mail system

VI. ALGORITHMS USED

There are several algorithms used for proposed system, which are mentioned as follows –

Breasman's Algorithm **–**It is useful for drawing circle for graphical scheme. Using circular schema we arrange all 64 characters in the 8 arce of the circle. Using this schema user easily login with

AES Algorithm – Using AES, we can perform encryption and decryption for security purpose.

VII. CONCLUSION

In this paper, we focused on design a system which Resistant the shoulder surfing attack and secure E-mail using encryption and decryption. The user can easily and efficiently login the system without using any physical keyboard or on-screen keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login

REFERENCES

[1] "A Simple Text Based shoulder surfing Resistent Graphical Password scheme" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE),2013.
[2] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," *Draft*, 2005.
[3] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget,"Design and evaluation of a shoulder-surfing resistant graphical password scheme," *Proc. of Working Conf. on Advanced Visual Interfaces*, May. 2006, pp. 177-184.
[4] B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," *Informatika*, vol. 7, no. 2, 2006, pp. 91-97.
[5] R.Anand[ll,R.Regan[2l, V.Mohanraj ," CLOUD BASED SHOPPING GUIDESYSTEM USING QRCODE" IEEE-201S0.
[6] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011.
[7] Pavlidis T, Swartz J. Fundamentals of information theory[J]. IEEE Computer, 990, 23(4): 74- 86.