ISSN No: - 2456 - 2165

Session Password Authentication using Magic Rectangle Generation Algorithm(MRGA)

Mrunal V. Arak Prof.D.T.Salunke Tanvi A. Merai Pooja B. Sutar

mrunalini1695@gmail.com dipmala.salunke@gmail.com merai.tanvi@gmail.com poojasutar54.ps@gmail.com

Information Technology, JSPM's Rajarshi Shahu College of Engineering, Pune, India

***Abstract*—Security is demanded in many ranges of applications. Mostly for authentication purpose user tend to use textual passwords. But they are vulnerable to dictionary attacks, shoulder surfing, eaves dropping, and social engineering. As an alternative to textual passwords, graphical passwords can be used. But even graphical passwords are vulnerable to shoulder surfing. So as to cope up with this problem we can combine text with images to generate session passwords. By using this the session passwords will be generated only once. In our project two techniques are used to generate session passwords using text and colors. When the session passwords is entered the innovative algorithm namely Magic Rectangle Generation algorithm (MRGA) is applied. The singly even Magic Rectangle is formed based on seed number, start number, row sum and column sum. The value of row sum and column sum is very difficult to trace. Hence it is helpful to enhance the security due to its complexity in encryption process.**

Keywords:- *Textual and Graphical Password, attacks, security, authentication,Magic Rectangle Generation Algorithm,, encryption*

I. INTRODUCTION

In the world of Internet, organizations are becoming more and more dependent on information system. Threats to the information system are increasing and hence, there is a need to protect the information that is being transferred between the individuals through the internet. Cryptography is the study of hiding the user information which is used for identification and authorization of user.

For authentication and authorization purpose the most common method used is the textual passwords. Authentication is a step by step process of providing credentials to authorize the users to gain access to the resources. The passwords always play a significant role in providing security and authentication to every user, so it is necessary that password selection should be appropriate. These passwords must be secured by encryption process to enhance computer security for protecting it from attacks. The issues related are eaves dropping, dictionary attack, social engineering and shoulder surfing. Random and variable length passwords can make the system secure but the main problem arises with the difficulty in remembering these passwords. Unfortunately, these passwords are easily cracked. The other available techniques are graphical passwords. There are many graphical password schemes which brought into existence in last few year but these passwords are suffering from shoulder surfing which is a major issue.

To overcome these issues of the textual and graphical passwords, in this paper we present the technique of combining these two types of passwords which provides high level of authentication. To implement this idea we use pair based authentication and hybrid textual authentication technique using colors and session passwords.

II. LITERATURE SURVEY

User has to select a set of images from a set of random images during registration and then during login the user has to identify those preselected images for authentication. This system is vulnerable to shoulder-surfing. [1]. The user has to re-draw the pre-defined picture on a 2D grid and if the drawn picture touches the same grids in the same sequence, then the user is said to be authenticated. But this DAS scheme is vulnerable to shoulder surfing too. [2]. Proposed a graphical password entry scheme using convex hull method against shoulder surfing attacks. User must be able to recognize passing objects and click inside the convex hull formed by these passing objects. If user wants to make the password hard to crack, large set of objects can be used but this objects will make the images look very crowdy and the objects almost indistinguishable. Using fewer objects may lead to a smaller password space resulting convex hull to be large [3].Designed a graphical password scheme where the user has to click on the approximated areas of pre-defined locations on particular image[4]. To avoid or to reduce threats of the shoulder-surfing problem, one technique was developed by Zhao and Li named as "S3PAS". The importance behind this scheme is in the login stage, where the original text passwords in the login image must be found out and clicked inside the invisible triangular region. The system has both graphicaland textual password scheme integrated in it and has high level security. Scheme rows perfect results it requires the user to remember code along with the pass-object variants [5,6,7].

III. SYSTEM ARCHITECTURE

The following fig.1 explain the architecture of system

ISSN No: - 2456 - 2165

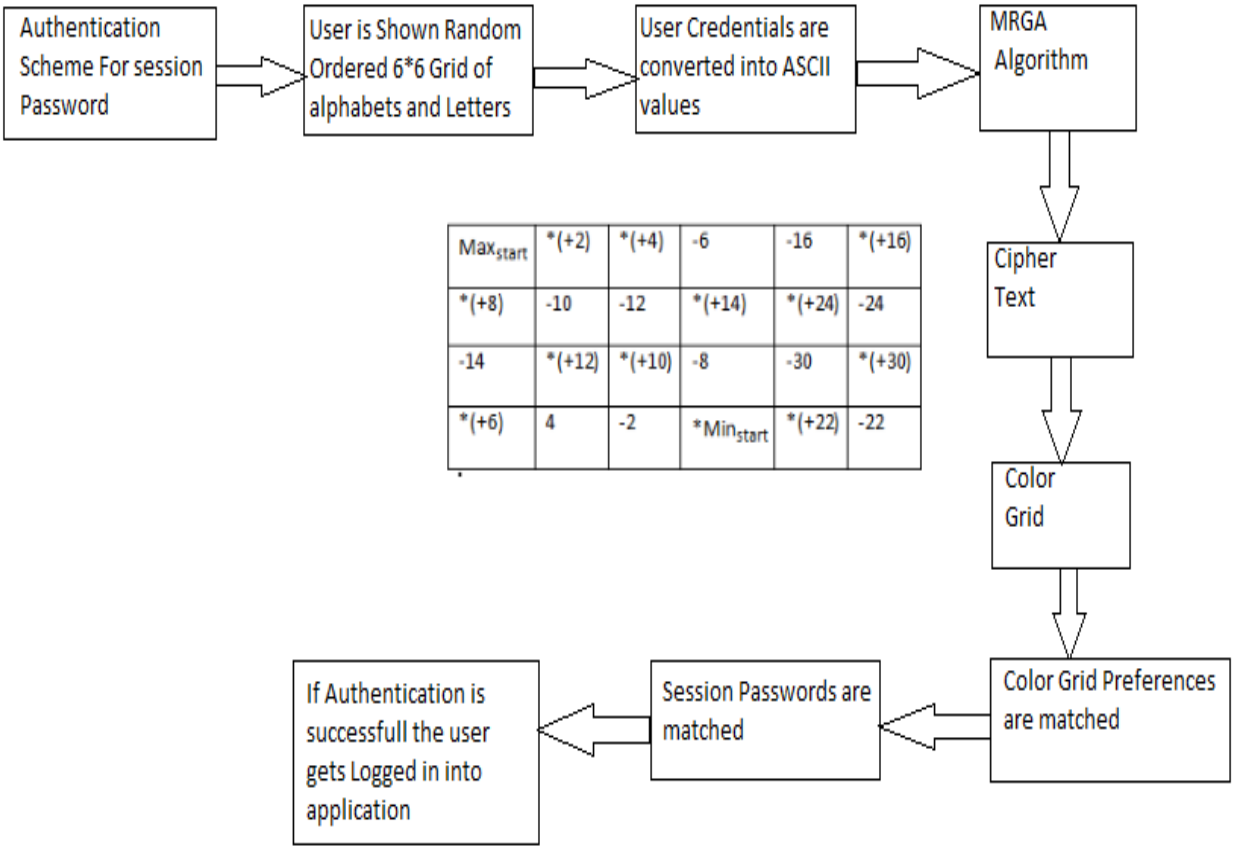

fig.1 Architecture of the system.

The user (registered) begins with the login interface where user gives its login credentials like username and the passwords as input which is generated by 6 x 6 grid. The passwords are the send to Magic Rectangle Generation Algorithm(MRGA) which converts the numerical value into ASCII value. The ASCII value is then encrypted which is the cipher text. The user is then showed next interface consisting of colors based on the ratings given by the user at the time of registration. The user enters the color password and at the server side the color preferences and session passwords are matched. Finally when the passwords are matched and authentication is done the user is able to access the application securely.

The following are the two levels used for authentication:

A. Pair-based Authentication scheme.

- *Registration*

During registration user has to submit his original password which has maximum length of 8 characters and it is also called as secret pass, it should contain even number of characters. Session passwords are generated based on this secret pass.

- *Login*

During the Login phase, user enters his username. An interface consisting of grid is displayed which is of size 6 x 6 and it consists of alphabets and numbers as shown in fig2. These are randomly placed in grid form and the interface changes every time. User needs to enter the password depending upon the secret pass. User considers his secret pass in terms of pairs of two characters each.

- *Session Password Generation Process*

The session password is made up of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter of row and column is part of the session password which repeated for all pairs of secret pass.The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 36^8.

Fig.2.Login phase for Pair Based Authentication

ISSN No: - 2456 - 2165

B. Hybrid Textual Authentication Scheme

- *Registration*

The User should rate colors from 1 to 8 and he can remember it as "BIGCROPS". Same rating can be given to different colors as shown in fig.3.

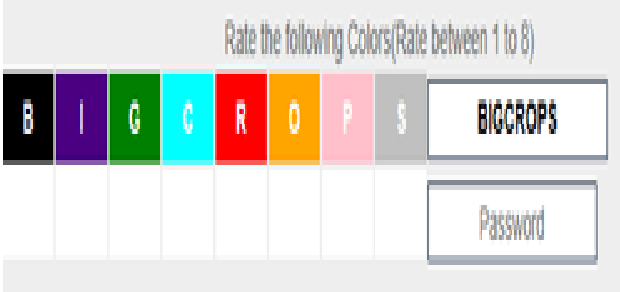

Fig.3. Registration Phase of Hybrid Scheme

- *Login*

During the login phase, interface consisting of colors is displayed based on the colors selected by the user as shown in fig.4.The login interface consists of grid of size 8×8 which contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. Depending on the ratings given to colors, we get the session password.

Fig.4.Login phase of Hybrid Scheme

IV. MRGA ALGORITHM

A. Steps of Algorithm

- First step deals with the construction of different singly even magic rectangle that contains total 1536 values and been divided into 12 quadrants, each consists of 128 characters which is of order 32x48 and then it is used in ASCII table with 128 values.
- Second step deals with each character of the plain text that is been converted into numerals based on its position in magic rectangle in different quadrants. The numerals are then encrypted and decrypted.

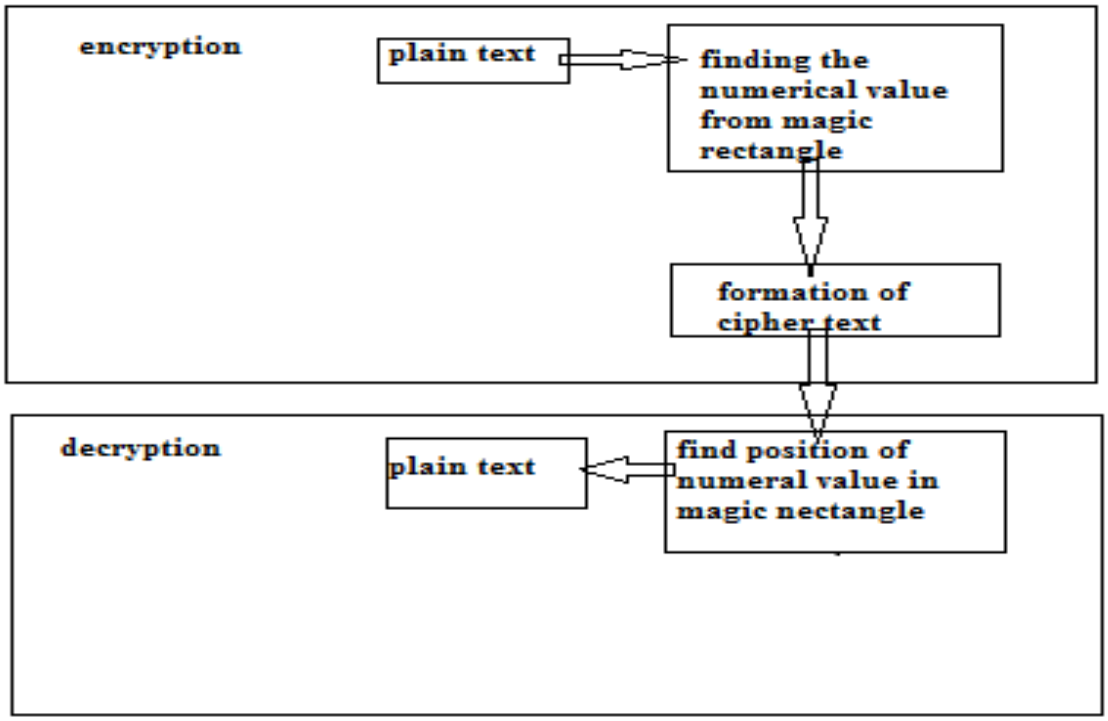

Fig5.working of algorithm

ISSN No: - 2456 - 2165

B. Construction of Magic Rectangle

The base for Magic rectangle is the magic square of order n which includes the organization of integers in form of n*n matrix such that the sums of all the elements in every row, column is equal .Along with it is also necessary that, the sums of all elements along the two main diagonals are also equal. The magic constant of a magic square depends only on n and has the value **M (n) =n (n2+1) / 2**.

The basic requirement in formation of Magic rectangle is that sums of all the elements in every row as well as columns are to be equal. The order of the matrix is even but not divisible by four such as 4x6, 8x12, 16x24, 32x48 etc.

In general, m*n rectangle a=m and b=n i.e. one a*a matrix and increases by b columns

$$(a+b)/a \equiv a/b \qquad .....(1)$$

- *Function used*

For construction, divide and Conquer method is used. The initial input column sum is fixed as 32x48 which is then divided by two to form the next level of magic rectangle which is in the order of 16x24. The resultant column sum is further is divided by two to obtain the next level of MR which is in the order of 8x12.
The column sum is calculated by the below formula

$$MR_{i*j}csum = (csum / n) \qquad ....(2)$$

where,
n=2,4,8,….
i=x,x/2,x/4,x/8….
j=y,y/2,y/4,y/8…

x and y may be any positive integer divisible by four. MR_{ixj} represents the row(i) and column(j) of the Magic Rectangle MR.

The row sum is calculated by using the following formula

$$MR_{i*j}rsum = csum + (csum / n) \qquad ....(3)$$

where
n=2,4,8,….
i=x,x/2,x/4,x/8….
j=y,y/2,y/4,y/8…

If the initial input column sum is taken as even value, then it matches exactly in column sum of magic rectangle. On the other hand, if the column sum is taken as odd value, then the resultant column sum to be reduced by one because of fractional value. Here the singly even magic rectangle is generated by using any seed number, starting number and magic column sum. In consecutive order the numbers are generated.

The values in the Magic Rectangle(MR)4x6 are filled as shown in Fig.6.

The function is called MR4x6 fill order (Minstart, Maxstart).

Max_{start}	*(+2)	*(+4)	-6	-16	*(+16)
*(+8)	-10	-12	*(+14)	*(+24)	-24
-14	*(+12)	*(+10)	-8	-30	*(+30)
*(+6)	4	-2	$*Min_{start}$	*(+22)	-22

Fig.6. Magic Rectangle

where '*' in magic rectangle are places to be filled having its starting point from Minstart and incremented by 2 each time to get the next number. The places where there is no '*' in magic rectangle to be filled having its starting point from Maxstart and decremented by 2 to get the next number.

The MR algorithm started with the input values Minstart, Maxstart, column sum and seed value. The seed value is the 4 bit binary value. If the input seed value is '1' bit, then either row or column of Magic Rectangle is shifted circularly, Otherwise the shift of row or column is not warranted.

1) Read seed number, Minstart, Maxstart value and Initial column sum.
2) Compute the row sum and column sum.
3) Generate the magic rectangle.
4) If (seed number == 1)Shift either row/column Else step 2.

This will create four magic rectangles. These four MR are combined together to form the next level of MR by using the following method

$$MR_{i*j}=MR_{(i/2)*(j/2)}||MR_{(i/2)*(j/2)}||MR_{(i/2)*(j/2)}||MR_{(i/2)*(j/2)} \qquad ...(4)$$

C. Advantages of Using Magic Rectangle

Each communication session uses a newly generated Magic Rectangle which increases the randomness of the cipher text value even though the characters are repeated. Can Generate rectangles from any values with equal row sums and column sums. No change in the encryption and decryption time using MR. Capable of applying MR in any Public key algorithms.

ISSN No: - 2456 - 2165

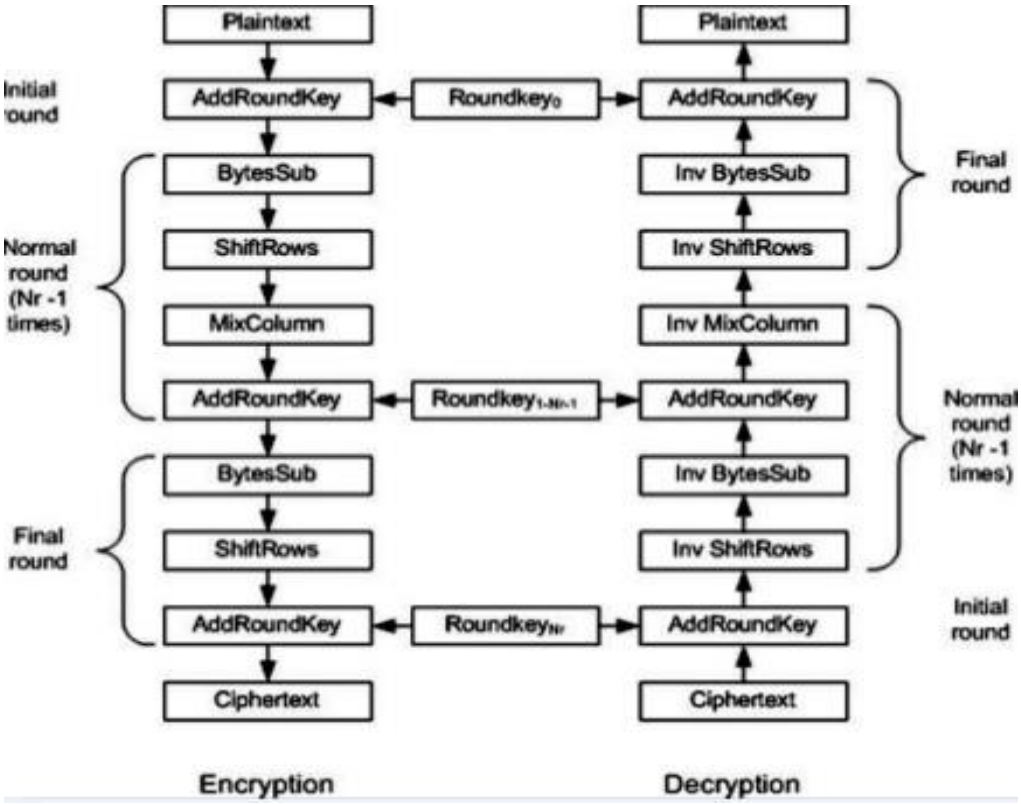

Fig.7.AES ALGORITHM

D. Encryption

The following AES steps of encryption for a 128-bit block:

1. Derive the round keys from the cipher key.
2. Initialize the array with the block data
3. Add the initial round key to the starting array.
4. Perform 9 rounds of state manipulation.
5. Perform the $10^{th}$and final round of state manipulation.
6. Copy the final state array as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state array.
steps involve four types of operations called:

1. Sub-Bytes
2. Shift-Rows
3. Mix-Columns
4. Xor-Round Key

- *Sub-Bytes*

This operation is a simple substitution that converts every byte into a different value.

- *Shift-Rows*

As the name suggests, Shift-Rows operates on each row of the state array. Each row is rotated to right by a number of bytes as follows:

1st Row:rotated by 0 bytes (i.e., is not changed)
2nd Row: rotated by 1 byte
3rd Row: rotated by 2 bytes
4th Row: rotated by 3 bytes

- *Mix-Columns*

This operation is the most difficult to explain and perform. Each column of the state array is processed separately to produce a new column which replaces the old one. The processing involves a matrix multiplication.

- *XOR-Round Key*

After the Mix-Columns operation, the Xor-Round Key is very simple and hardly needs its own name. This operation simply takes the existing state array, XORs the value of appropriate round key, and then replaces the state array with the result. It is done once before the rounds start and then once per round, using each of the round keys in turn.

E. Decryption

Decryption involves revere of all the steps taken during encryption using inverse functions:

1. InvSub-Bytes
2. InvShift-Rows
3. InvMix-Columns

Operation in decryption is

1. Perform initial decryption round:
   - InvShift-Rows

- Xor-Round Key
- InvSub-Bytes

2.Perform nine full decryption rounds:

- Xor-Round Key
- InvMix-Columns
- InvShift-Rows
- InvSub-Bytes

3.Perform final Xor-Round Key
The same round keys are used in the same order.

V. EXPERIMENTATION AND RESULT

The comparison between cipher text generated is shown in Table1

Existing AES			AES with MR		
Plain Text	ASCII Value	Cipher Text	Plain Text	MR Value	Cipher Text
S	83	194	S	1447	388
U	85	380	U	242	514
M	77	211	M	1395	134
M	77	211	M	1287	160
E	69	276	E	58	261
R	82	94	R	168	402

Table 1: Comparison of AES and AES with MR

In plain text, the character 'M' takes places twice. In existing encryption, the cipher text value of 'M' is same. In contrary, the cipher text value of the 'M' is 134 and 160 in the proposed AES with MR.

A. Security Analysis

Since the interface keeps changing every time, the session password also changes. It is a technique that is resistant to shoulder surfing. Because of dynamic passwords, dictionary attack is not possible.It increases the complexity to derive the plain text from the cipher text by any intruders.

VI. CONCLUSION

Various textual and graphical password authentication schemes are discussed in this paper which are vulnerable to security in some or the other way. Hence we come up with the new technique of combining both these types of passwords using Pair Based and Textual Hybrid schemes that proves to be robust. Pair Based and Textual Hybrid schemes provides two level of authentication to prevent against shoulder surfing threat and such kinds of attacks. Along with that we have used Magic Rectangle Generation Algorithm (MRGA), that generates new grid of 6x6 containing alphabets and numbers which help us generates new session passwords each time user login. In future, it is possible to come up with the new approach by analyzing all the discussed methods and find the efficient solution that would make the more user efficient schemes and reduces the time required for authentication.

REFERENCES

[1] R. Dhamija, A. Perrig paper based on Study Using Images for Authentication in 9th USENIX Security Symposium, 2000.

[2] JermynI, Mayer A., Monrose F., Reiter M. and Rubin. Study on Design analysis of graphical passwords in USENIX Security Symposium, August 1999.

[3] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon study on Design evaluation of a graphical password system. International J. of Human-Computer Studies 63 (2005) 102-127.

[4] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[5] H. Zhao and X. Li, "A Scalable Shoulder-Surfing Resistant Text and Graphical Password Authentication Scheme," in 21st International Conference on AINAW 07 vol. 2. Canada, 2007, pp. 467-472.

[6] S. Man, D. Hong, and M. Mathews paper on shoulder surfing resistant to graphical password scheme in International conference on security and management. Las Vegas, NV, 2003.

[7] Z. Zheng, X. Liu, L. Yin, Z. Liu study based on password authentication scheme using shape and text, Journal of Computers, vol.5, no.5 May 2010.

[8] D.I. George, J.Sai Geetha, K.Mani "Add-on Security for Public Key Cryptosystem with MR Column/Row Shifting"International Journal of Computer Applications (0975 – 8887) Volume 96– No.14, June 2014

[9] Dr. D.I. George Amalarethinam and Dr. D.I. George Amalarethinam"Enhancing Security level for Public Key Cryptosystem using MRGA" ,2014 World Congress on Computing and Communication Technologies.

[10]M.Arak,D.T.Salunke,T.Merai,.P.Sutar, "A Survey on Various Authentication Mechanisms using Graphical Passwords" International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 12, December 2016