International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

EADP: Enhanced Authentication using Novel Dynamic Password

Sarthak Gupta **Virat Singh Chauhan**
Sarthakanamika@gmail.com Chauhanvirat13@gmail.com
Dept. of Information Technology
Vellore Institute of Technology

***Abstract*-In today's modern age of Internet, gifted by technology, for verification of user, Password is used. Password is a collection of different characters exists in ASCII code (Text Based) or set of different control signal which is generated based on biological impression of human being (Biometrics). Existing work shows that both Text based password and Graphical password suffer socio-economic problems and internal security issues. By considering this issue, a new security method, Enhanced Authentication scheme using Dynamic Password (EDAP), has been proposed with two-fold; first fold uses Ratings (of Color or Alphabets) for user verification and the second fold uses mathematical matrix for dynamic password generation. In every login of session, user feeds new password, which is completely shielded from various attacks.**

***Keywords*- Dynamic Password, Rating, Matrix, List (python), Security, Dictionary attack, Brute force, Authentication, optimal, reliability.**

I. INTRODUCTION

Security is the major concerns in the era of Internet, with increasing number of Internet based services like cloud, big data analysis, E-commerce. User data has become important asset to every Internet based services provider. At the same time, it is equally important to protect user level classified confidential data and information from several malicious hackers intended to illegally acquire information that are not just meant for them. So, search for new methods that protect from this type of threats have begun.

Many authentication scheme and techniques have been developed to protect users from recent and forth coming evolving threats. One such scheme - oldest, widely popular and highly in used today is Textual passwords or Text Based Password. Text based password are those in which ASCII code characters are used, but this method is highly vulnerable to different attack techniques like brute force, dictionary attack, eves dropping, social engineering, shoulder surfing and even many more. Though complex and lengthy text-based password slightly increase the level of security but then it becomes very complicated for user to remember and recall it at time of application. Generally, users tend to select short and easy password like birth date, pets name, and spouse names. This is also a problem because this password can be easily guessed, calculated or cracked by hackers.

Authentication is the process of verifying the identity of a person and authenticating that "He is who he claims he is" considered as the best way. This is to reduce the probability that the requestor is presenting false evidence of its identity. The ways in which a user may be authenticated fall into three factors below: Two Factor Authentication is the approach to authentication using two or more of the three authentication factors. A system's authentication is strong when it requires at least two of the three authentication factors before users are granted access to the system.

Alternative to Text based passwords are the newly introduced Graphical passwords and Biometrics. But this technique also has its own shortcake and disadvantage. Graphical password provides assured high-level security but they are very slow in processing, expensive and require specific skilled operations. Biometrics/Cliometrics deals with finger prints, Retina scan or Voice/facial recognition this provide good security still they are not used because they are expensive and its authentication process is very slow. Many graphical passwords have been developed in the past decade which suffer peeking problems and shoulder surfing.

Thus, New authentication scheme have to be developed to provide impregnable security to user and to overcome the disadvantage of widely used Text Based or Graphical Password method. This paper claims that the implementation authentication of a scheme could increase security.

II. LITERARY SURVEY

Numerous sophisticated investigations on the authentication schemes have been done. And it has been discerned that none of the secure authentication schemes can prevent all sorts of attacks. With this temporary outcome, this paper proposes an authentication schemes

which overcomes all the existing problems in recent authentication schemes. Literary survey reveals some studies that are achieved in the past. Some of these schemes are discussed as follows:

- In year 1974, A.Evans Jr.,W.Kantrowitz, E.Weiss, "A user authentication scheme not requiring secrecy in the computer", Computer Society ACM, was a the first one who thought of creating the dynamic password generation or termed as OTP generation.
- In year 1996 C.J.Mitchell, L.Chen, Comments on the S/Key user authentication scheme explained about the system of matrices and how their involvement can help us to create more secured passwords, ACM Operating system.It has been reported that the password authentication scheme is vulnerable to many attacks, including stolen-verifier attack.
- In early 1990s, Jermyn introduced a technique called "Draw a Secret". In this technique user draw a picture as a password which is similar to drew parameterized registered password. For authentication drawn picture has to be match with registered drew picture on same grids in same order. It is vulnerable to shoulder surfing plus drawing picture as password is very complex task itself.
- [In early 1990s Zhao and Li invented a shoulder-surfing resistant scheme that makes different combinations of password and allow selection of appropriate middle symbol of invisible triangle as a password. It achieved good level of security. But selection of middle symbol in large triangle was difficult task.
- In year 2000according to Dhamija and Pirie Scheme of Image selection, User selects a set of images at time of registration and at time of login, user choose same images to authenticate. But this scheme was vulnerable to Shoulder surfing.
- In late 2000, Pass Face technique was developed by an American Firm Real User Software Inc., in which User has to select 4 familiar faces from a set of pictures of human face at the time of registration. At time of login User has to choose to select each face from interface of 3X3 Matrix, 4 times. In this method, it is quite confusing to remember which face is correct and this technique can be easily cracked by just guessing.
- In the year 2005, Balaji .R, Roopak. V made RSA security selected by national bank of Abhu Dhabi to protect online banking customers where the user will be provided the OTP by certain secure means , which can be password scratch sheet or security token.
- In year 2006, Jong-Won Seo ,Je -Gyeong Jo ,Hyung-Woo,"SMS(Short Message Service)"
- Based secure authentication and accounting Mechanism in Wireless and Accounting Mechanism in Wireless network ,"Hybrid Information Technology ,2006",International Conference.
- In the recent years 2011, D.Pansa, T.Chomsiri,"Web security improving by using dynamic password authentication", International conference on network and Electronics Engineering.

III. MATHEMATICAL BACKGROUND (MATRIX)

The Mathematical Background used in the EADP is Matrices. During the generation of EADP the ASCII characters are stored in a dynamically generated Random matrix which makes the system of security more enhanced as for each iteration the matrix is reshuffled and thus the encryption can't be decrypted easily.

Thus it increases the security of the password generated by the program that is by picking up the different elements from the matrix and the matrix at each iteration will get updated by the use of the RANDOM function making the password more secure. We can take the example of matrices generated of different sizes so that we can show its elements which have been taken as the input in the matrix and for the security analysis.

1. If we take the matrix of 8X8

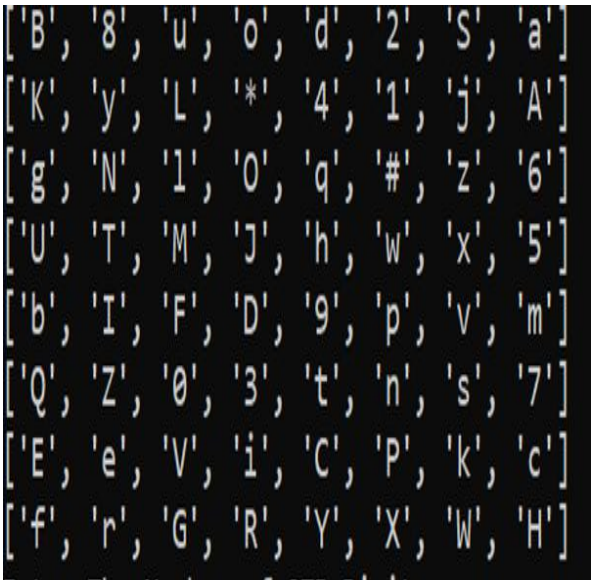

Figure 1 Sample randomized matrix generated for 8x8.

Then the number of elements that can be inserted are 64 [8X8] elements that includes the special characters [!,@,#,$,%,^,&,*] all Case Sensitive letters and numbers. This OTP generation method has been used in the program using Random function so that at each iteration it will change the order in the matrix with respect to the previous location and thus increasing the security.

2. If we take 12X12 matrix

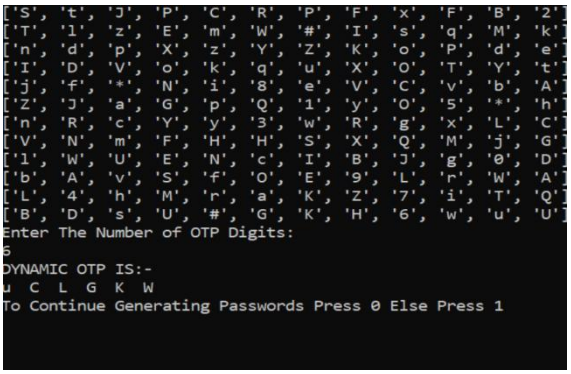

Figure 2 Sample randomized matrix generated for 12x12.

The 12X12 matrix includes 144 distinct elements with higher security purpose as you can see in the code the Dynamic OTP generated is more secured as compared to the 8X8 because of more elements and higher randomness.

3. If we take 16X16 matrix

Figure 3 Sample randomized matrix Generated for 16x16.

If we take 16X16 matrix it can include 256 number of elements having more security and insures more dynamically generated OTP generation. It can also be used in the Bank Security system and other sectors as well for security analysis.

IV. EXECUTION AND EXPERIMENTAL RESULTS

1.Proposed Algorithm

Code for the Random Matrix Generation and DYNAMIC OTP:

Algorithm:

- Creating List.
- Inserting alphabets, number using (append) and special characters of their
- Respective ASCII notation in a list by loop.
- Using Random function inserting elements in a Matrix(8*8), elements will be inserted into the freshly assigned or reshuffled position in the matrix by using the RANDOM function as explained in 4.2.
- Getting input of number of digits in OTP.
- Using random function selecting integral coordinates of form (i ,j) where
- 0<=i<=7 ,0<=j<=7 for each digit in OTP.
- Fetch the corresponding element from Randomized matrix.
- Print the corresponding OTP.

2. Enhanced Authentication using Dynamic Password (EADP)

The proposed authentication is carried out using Dynamic password. Dynamic password changes each and every time the user logs in. It means once the session is expired the newly generated password is destroyed and no longer useful. For every Session, users input different password that provide enhanced security against straight forward approach attacks like Brute force and dictionary. This method uses Randomized Matrix for generating Dynamic password. During Login the User enter the username and password and proceeds the user is further required to enter mobile number on which a Dynamic OTP is generated using Randomized matrix.

The matrix has total of 64 elements i.e. 8X8 matrix which includes ASCII characters (A-Z),(a-z), (0-9) and (#, *) as Special characters. The matrix is randomized on every session which makes the position of every element change on session. The characters picked from this dynamic matrix are also randomized i.e. If (i, j)th element is taken from the matrix i belongs to range(0-7) and j also in range(0-7). For this each pair the (i.j) values are randomized. Thus for each time random matrix creation total possible combinations for each OTP digit is(8X8X(64^64)) which makes the total combinations for a n digit OTP be (8X8X(64^64))^n. Here is the explanation of the Steps involved in the Program.

Step 1- First through the creation of the 2-D lists different elements are being inserted into the matrix by their different ASCII code where it gets converted are being inserted with the help of the loop [for loop used in the program].

Step 2-Then the input of 6 characters OTP is being asked from the user then the pointer goes to the code picks up the different characters from the different locations using the Random Function as being requested by the Server.

Step 3- In the next iteration by the Random function the elements in the matrix will be assigned fresh and newly generated position in any order assigned accordingly.

Step 4- With the use of the pointer variable if another request is being made by the user for generating the OTP then the pointer after getting request from server will again examine each element in the matrix and will randomly pick freshly assigned position from the matrix.

Step 5-Flag variable is being used in the program and being included in the loop for asking the request to again generate the Dynamic password.

3. Random Number Generation

Backbone of proposed method is based on the generation of random number which will manipulate representation of rating as well as element of grid which are further

considered as password digit hence it is very crucial to decide and implement the algorithm which is efficient.
Sample Python program to generate Random Number within range without repetition:

```
# Program to generate a random number between a and b
# import the random module
import random
a=int (input ('Input a value'))
b=int (input ('Input b value'))
print (random.randint(a,b))
```

4. Program Explanation

The code uses the python built-in function random.randint(a,b). random.randint () is used to generate a random integer between 2 numbers.

In code a ,b are variables which are taken as input from the user and a random number is generated using the function in python. The random.randint() function uses "Mersenne Twister" technique to generate a random number in a given range.

5.Testing Constraints

- Python language
- Generation 512KB of Random Number
- Run 100 Times and Average is Calculated(Floating point)

6.Testing Environment

- Intel Core–i5 Processor
- 8GB RAM
- 64 bit Windows 10

7. Strength and Soundness of EADP:

- The EADP uses "Mersenne Twister" technique to generate random matrices which is by far the most widely used general-purpose PRNG (Pseudorandom number generator.) The technique was developed by Makoto Matsumotoand Takauji Nishimura in 1997. This technique has Passed numerous tests for statistical randomness, including the Diehard tests.
- The EADP uses the above technique to generate Random 8X8 matrix of ASCII characters which makes it almost impossible to find an encrypting pattern in EADP. Also, this Random matrix is backed with randomness in choosing (i, j) pairs in the nth digit EADP.
- EADP is Dynamic and the password is destroyed as soon as the verification is done thus the encryption pattern is impossible to trace.
- For Each User session the Dynamic password can only be traced by the server once i.e. no traces are left after the session is expired. On Re-Query the System against generates a new EADP and the old EADP is destroyed.

8. Security Analysis of EADP Scheme

8.1 Brute force attack-This method completely prevents brute force because password will be changed in every login.

8.2 Dictionary Attack- These are attacks directed towards character string password. In this attack, hackers use the dictionary words and authenticate by trying one word after another in sequence. The Dictionary attacks fails towards our proposed scheme because dynamic passwords are used for every login.

8.3 Shoulder Surfing- In proposed scheme the randomized strips of alphabet hide the password and Matrix elements are also randomly generated, hence completely resistant to Shoulder surfing or hidden camera. Even if someone knows the password, it has been already changed in new session and it is impossible to generate new dynamic password unless rating is known.

8.4 Guessing- It is not at all possible to guess the dynamic password because displayed strip will be randomized with random placement of numbers matrix in the log in interface.

V. FLOWCHART OF EADP SCHEME

First it will be verified whether user is registered or not. If yes, then proceed to log in, but if user is not registered then process of registration to be done, then to the log in step. Once the user enter the password and it matches with the database the user needs to enter mobile number. At the same time an EADP password will be generated by the server which will be sent to the phone number of the user which will be then verified by the server on query.

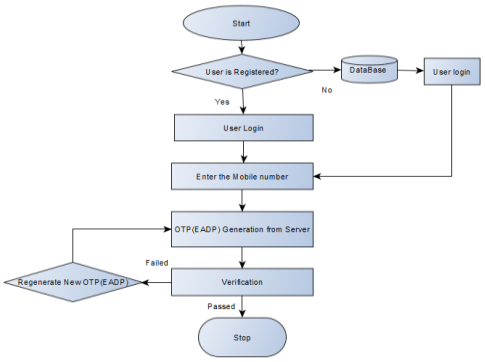

Figure 4 Program Flow.

Flow chart of EADP process with Server site and Client side phase as a collaborated system for Authentication.

1. Program:-

```
flag=0
while(flag==0):
import random
q=[]
 a=[x for x in range(65,91)]
 for f in range(48,58):
a. append(f)
 for e in range(97,123):
a. append(e)
a. append(35)
a. append(42)
 matrix=[]
 for i in range(0,8):
```

International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

```
in Array=[]
for j in range(0,8):
c=a [random.randint(0,len(a)-1)]
a. remove(c)
in Array. Append(chr(c))
matrix. Append (in Array)
print("Enter The Number of OTP Digits:")
num=int(input())
for r in range(num):
 l=random.randint(0,7)
p=random.randint(0,7)
q.append(matrix[l][p])
print("DYNAMIC OTP IS:-")
for k in q:
print(k," ",end="")
print("\nTo Continue Generating Passwords Press 0 Else Press 1")
ch=int(input())
 if(ch==0):
 flag=0
elif(ch==1):
 flag=1
```

2. Program Explanation-

Variable used in the program are flag, q, k, ch, r, x, a.chr(x) represent a function to fetch the ASCII value of corresponding integer. Where 'a' represent a 1D list which contains the total of 64 elements which are randomly picked and are append on Matrix (2D List). For a input 'num' i.e. number of OTP digits i, j values are randomly generated in a range of (0-7) for each character in OTP new element is picked up from the matrix. These characters are stored in a list which is the required OTP.
The process is repeated for each session until the value of flag is set to 1The Sample Output for 6-digit OTP is mentioned below: -

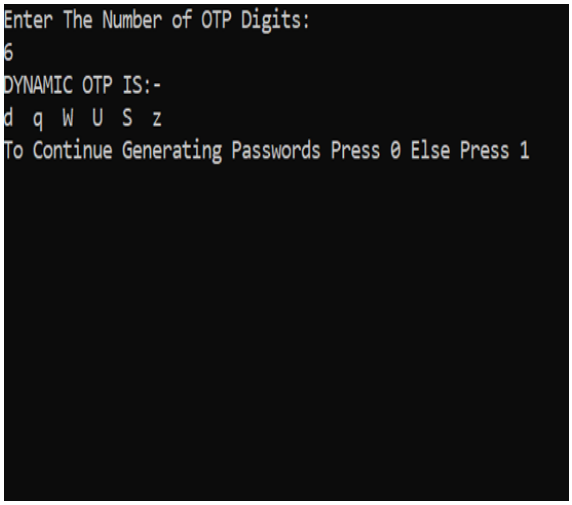

Figure 5 Sample OTP Generated for 6 digit input.

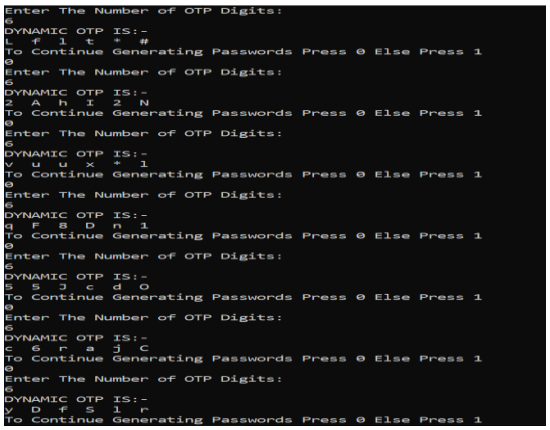

Figure 6 Sample OTP Generated, repeated for 1000 iterations.

3. Experimental Results

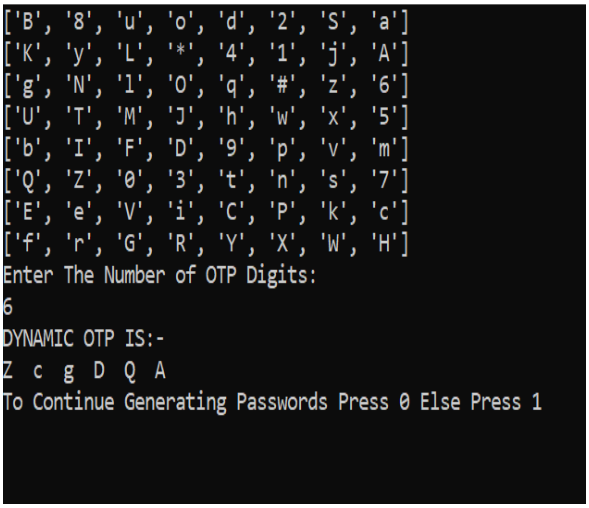

Figure 7 Experimental Result 1.

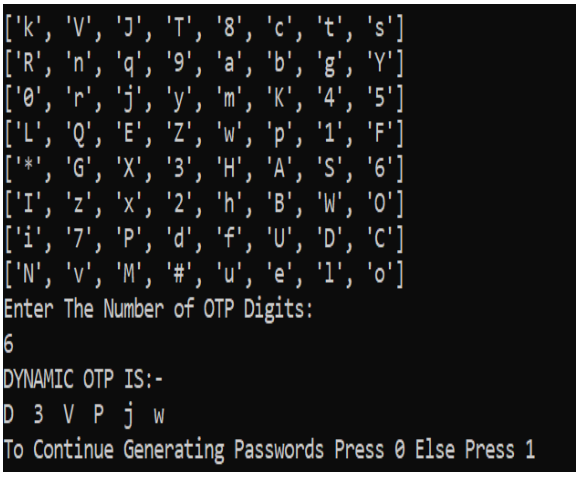

Figure 8 Experimental Result 2.

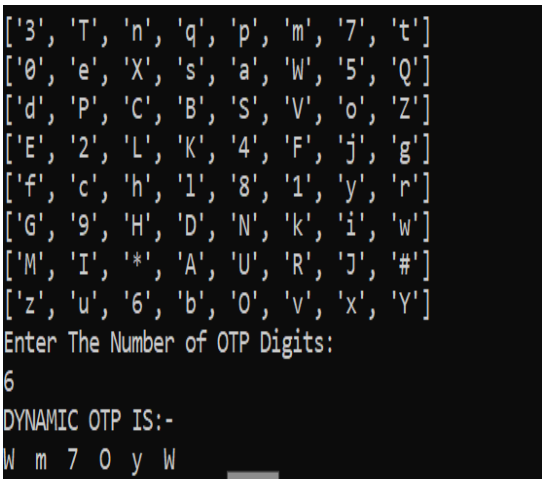

Figure 9 Experimental Result 3.

VI. CONCLUSIONS

Generally, there are lots of disadvantage in Text Based and Graphical authentication scheme. They are vulnerable and extensively open to several security attacks. As such, I have proposed the idea of dynamic password scheme which is capable of completely preventing attacks like Brute force, Dictionary attack, Guessing and Cracking and Shoulder surfing.In the future, the encryption of rating stored in the database can be done using rijndael's algorithm (Candidate of A.E.S), so in case if the Hacker/Attacker got access to the database the corresponding data is meaningless unless it is decrypted by the code which present at the application side, hence preventing SQL injection Attack.

This Method can be used in windows application such as a folder locker or an external gateway authentication to connect the application to a database or an external embedded system device. In India, this authentication scheme is not used in any Internet based - banking application. So, the banks can adopt this authentication scheme for improving their security. Besides this, the EADP scheme can be used in Military Companies to store their secret data and in any other application where security is the main concern. The EADP can generate password of 'n' number of characters thus is could be used to encrypt highly valuable information to improve the security in Information Technology field.

REFERENCES

[1] Dhamija and Perrig "A Study Using Images for Authentication". In 9 th USENIX Security Symposium, 2000.
[2] H. Zhao "A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 31st International Conference on Advanced Information Networking
[3] Xiyang Liu U Zhongjie Ren, Haichang Gao XiulingChang:A New Graphical Password Scheme Resistant to Shoulder Surfing.
[4] V Kumar M Anirudh, MD Sultan,OTP International Journal of Network Security & Its Application(IJNSA),Vol.3, No.3,May2011.
[5] Blonder. Password Based on Graphics. United States Patent 5559961, 1996.
[6]Real User Corporation: Passfaces. www.passfaces.com
[7] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[8] W. Jansen, "Authenticating Users on Mobile Devices in Proceedings of Information Technology Security Conference, Toronto Canada,2003.
[9] S. Man, Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on Management and Security. Las Vegas,2004
[10] Suo, Zhu and Owen, "Graphical Passwords: A Survey". In Proceedings ACSSAC'07.
[11] Jermyn, Monrose, Reiter, and Rubin., "Design and analysis of graphical passwords "in Proceedings of USENIX Security Symposium, August 1999 Vol. 2, No. 3, pp. 73-75, 1999
[12] Zhang, Wu, Rigid Image Registration by PSOSQP Algorithm, Advances in Digital Multimedia, vol.2, no.2, pp.48, 2014
[13] Aruna Kumari, Gowtham, Rama krishna,Lalitha Surepeddi, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.4, no.3, pp.43-49, 2013
[14] Vikram Varma, Siva Pillalamarri Prasad,Leela Kumari, Virtual laboratory through internet, Advances in Information Technology and Management, vol.2, no.2, pp.62-65, 2013Some samples of these dynamic matrices: