File Sharing Approach using Encrypted ASCII Segmented Image Grid OTP

[1]Dinesh Kumar, [2]Manish Sharma
[1]PG Scholar, [2]Associate Professor
[1]Department of Computer Engineering & information Technology, Suresh GyanVihar University, Jaipur (India)
[2]Department of Computer Engineering & information Technology, Suresh GyanVihar University, Jaipur (India)

Security is the primary concern when sharing the data, whether the simple text files, image file or any textual information. The security concern is increasing day by day as the attacks on the information crucial to individual or the organization is also increasing day by day. The various authentication and password schemes are available for the protection of data, but all have some sort of loopholes. So , in order to further enhance the security level , we proposed the new graphical grid based scheme based on the image segmentation and ASCII value arrangement to form the more secure OTP , having novel characteristics which make it difficult to crack. In order to further raise the secure the generated pattern is again encrypted using HASH algorithm and key to further raise the level of security.

IndexTerms - Data Security, OTP, Grid Password.

I. INTRODUCTION

Password strength is a proportion of the adequacy of a password against estimating or savage drive ambushes. In its commonplace shape, it checks what number of preliminaries an attacker who does not have direct access to the password would require, all around, to get it successfully. The strength of a password is a part of length, diverse quality, and unpredictability[1].

Using solid passwords cuts down general threat of a security break, yet solid passwords don't swap the necessity for other feasible security controls. The viability of a password of a given strength is emphatically directed by the arrangement and execution of the factors (information, proprietorship, inherence). The essential variable is the major fixation in this article.

The rate at which an aggressor can submit conjectured passwords to the structure is a key consider deciding system security. A couple of systems drive a period out of a couple of moments after a humble number (e.g. three) of failed password entry attempts.

Without various vulnerabilities, such structures can be effectively secured with tolerably fundamental passwords. Anyway the system must store data about the customer passwords in some shape and if that data is stolen, say by breaking structure security, the customer passwords can be at possibility [2].

One-Time Password (OTP) is an advanced authentication scheme which offers exactness, security and secrecy. OTP Two-Factor Authentication is considered as one of the promising strategies in any web-empowered data system. As of now, there are numerous schemes have been created to defend and secure secret data. In any case, they vary from practical properties, strategies and materials utilized. Every one of which has exceptional methodology in taking care of dangers and attacks [3].

Grid authentication factor is about XY arrange query system. The arbitrary cell in the grid conveys the right blend of numbers and letters in the cell. A case of grid authentication scheme is the bingo card. It is a less secure options as a result of the three digits utilized less than most arbitrary OTP schemes and can be photocopied making it presented to dangers [3]. In any case, grid authentication is one of the intriguing authentication schemes that can be investigated to boost the arbitrary age of codes with numerical calculation and algorithmic scheme.

The expanding prevalence and utilization of OTP filled in as the best inspiration of this exploration think about. In spite of the fact that there is no best way to deal with secure authentication, this investigation will dissect and look at the changed methodologies OTP for grid authentication to figure out which of these schemes gives better execution, spares memory assets and gives quality key age. As needs be, the outcomes created by OTP are extraordinary thinking about its intricacy and randomicity.

II. RELATED WORK

Somwanshiet. Al 2017 [4] Textual secret key is most generally utilized authentication system for anchoring these applications. Authentication schemes are helpless against different kinds of attacks. The proposed system gives answer for the attacks in particular, 'Keystroke Logging', 'Shoulder Surfing' and 'Copy Login Pages'. The system enhances login security component. The system comprises of 6X6 framework of 26 letters in order and 10 digits to enter the secret phrase. While enlisting in the system the client need to give his private key which will be utilized while entering the secret phrase into the framework. The private key of the client will never be utilized anyplace thus there are no odds of getting the secret word broke.

S. Pandey, et. al, 2013 [5] In this paper, we examine how to keep clients' passwords from being stolen by enemies. Printed based secret phrase authentication scheme have a tendency to be more defenseless against attacks, for example, bear surfing. To conquer the vulnerabilities of conventional techniques, visual or graphical secret key schemes have been created as conceivable elective answers for content based scheme. Be that as it may, just embracing graphical secret word authentication additionally has a few downsides; henceforth some cross breed schemes dependent on content and in addition designs were produced. We propose a virtual secret phrase idea including a little measure of human processing to secure clients' passwords in on-line conditions. We

likewise break down how the proposed scheme safeguards against phishing, key lumberjack, bear surfing, man in the center and session seizing attacks.

S. Agrawal , et. al , 2016 [6] Security system assumes a crucial job in any system where client id involves concern, security systems are fundamental for any modernized or advanced access control. Authentication system have just been embedded for every one of the fields, for example, protection, data systems and even in physical structures .The proposed scheme plans to improve the unwavering quality of content based passwords for cutting edge clients by adjusting a mix of content and graphical passwords. Along these lines a more secure way will be given to clients to allowing access to a verified system. The proposed thought could be exceedingly helpful for ATM machines where get to technique is by means of a fake secret phrase.

M. H. Zaki ,et .al ,2017 [7] Text-based secret phrase authentication scheme is powerless against numerous attacks, for example, bear surfing attack and comparable sort of attacks like word reference attack, savage power attack and so on. Numerous realistic based secret word authentication schemes are there however they are additionally very costly in sending and needs more reaction time at login stage. In this paper, a more secure example key based secret phrase authentication scheme is proposed which gives greater security utilizing mix of example, key, and sham digits. For this, client needs to perceive and enroll design as area numbers from lattice, enlist key qualities that maps esteems to secret phrase and add sham qualities to secret phrase in order to mislead the attacker. From that point onward, to login, client needs to review the example and maps the printed secret word from example with enrolled key qualities, making a secret phrase by including sham digits. It limits the shoulder surfing, animal power attacks and so on because of high many-sided quality of speculating secret phrase in multi-levels: first from example, at that point from key and after that from sham qualities. This scheme is impervious to ease of use issues with the end goal that it doesn't over-burden human memory and gives additional security against unknown attackers.

R. Balaji and V. Roopak ,2011 [8] The fruitful check of a client or a substance wishing to utilize a PC based data system, lies at the center of the security of the systems. In spite of the fact that countless confirmation procedures have been proposed, secret key based strategies remain the prevalent strategy for decision. Hence, it is basic that these strategies be as compelling as could be expected under the circumstances. The customary secret phrase authentication system is confined by set of tenets like it ought to be of least 6 characters in length, ought to contain alphanumeric characters and even with extraordinary images. The traditional secret phrase system is highly secured except if until the point that the secret word isn't known to other people or it isn't hacked by any programmer. On the off chance that the secret phrase is known to anybody other than the first record holder, he/she is allowed to sign in to the record and view individual data or imitate the genuine proprietor. Subsequently an elective strategy ought to be composed so the security and credibility is kept up. Consequently we propose a thought which utilizes dynamic secret phrase system for authentication and subsequently security and accordingly giving a powerful and effective answer for the above said issue.

III. Proposed Work

Step 1 : The proposed concept is using the 9X10 grid , in which are using the concept of scrambling the images , so the concept work in the following manner,

Firstly , the 9X 10 grid which is empty

Fig 1 Grid Structure

Step 2: Secondly, the user is provided with the set of images from which the user selected

Fig 2 Image Set for Segmentation

Suppose that the user choose the image

Fig 3 Selected Image

Step 3: Then in the next step image will get segmented,

Fig 4 Segmented Image

Step 4: Now the grid is arranged with the characters corresponding to the block number in the grid as the visible characters start from the ASCII value 40 , so plus 39 in the each block position

(	)	*	+	,	-	.	/	0	1
2	3						…..		
								€	

Fig 5 ASCII Representation in Grid

Step 5: Now, the segmented images are arranged in the pattern , which the user want , the user have to just drag the part and place that dragged part in the grid ,

(	)	*	+	,	-	.	/	0	1
2	3						… ..		
								€	

Fig 6 Segments Image Placement in Grid

So , now the password word pattern which will get created will be , mi-Segment-1-1-(-mi-Segment-4-7-.-mi-Segment-3-9-0-mi-Segment-2-11-2-mi-Segment-5-12-3-mi-Segment-6-89-€-, it will be password which is used for the accessing the shared file.

Step 6: Encrypt the OTP /Password using the Hash Algorithm and the key and store the information in the database

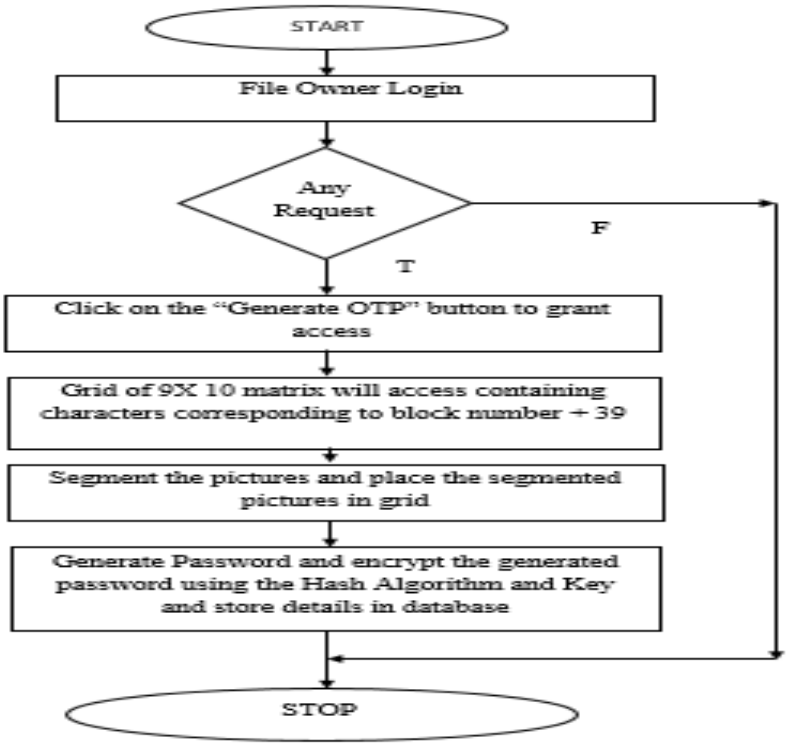

Fig 7 Flowchart for proposed approach

IV. Result Analysis

We have tested the KEY generated by our proposed implementation using the various tools to check its strength. Below is presented the some of the test analysis presented on the KEY.

A. Password Meter:-

The site www.passwordmeter.com is an online website which tests the strength of the password. This application is intended to evaluate the strength of password strings. The prompt visual feedback gives the client an approach to upgrade the strength of their passwords, with a hard spotlight on breaking the ordinary negative standards of conduct of imperfect password itemizing. Since no official weighting system exists, they made equations to overview the general strength of a given password.

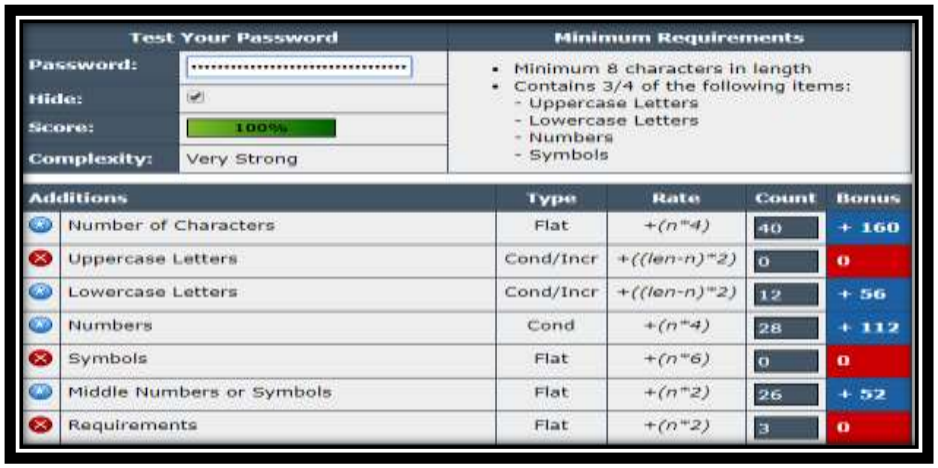

Fig.:-8 Test Results for website www.passwordmeter.com

The test password which is given is,

KEY: ba-Segment-1-1-(-ba-Segment-2-3-*-ba-Segment-6-10-1-ba-Segment-3-15-6-ba-Segment-4-17-8-ba-Segment-5-27-B-
Result: Very Strong

B. Password Checker

Password Checker Online encourages you to evaluate the strength of your password. Simply more absolutely, Password Checker online checks the password strength against two essential sorts of password breaking strategies – the savage compel strike and the word reference attack. It likewise analyzes the etymological structure of your password and lights up you about its possible deficiencies. This instrument can thusly likewise enable you to make more grounded password from a weak one.

Fig. 9 Test result for OTP online

C. CryptTool2

CrypTool is a program for learning cryptographic calculations. It gives a graphical UI to visual programming. Thusly, work processes can be pictured and controlled to enable intuitive control and association of cryptographic functions. The vector-arranged GUI relies upon the Windows Presentation Foundation (WPF) and enables clients to scale the present view unreservedly.

Fig. 10 Test Result using Cryptool2

The Fig. 4.3 shows the test result obtained using the Cryptool2.The above tests can be summarized using the table 4.1, which shows the result of the Key strength using the three tools which we have taken for the testing purpose.

TABLE 1 TEST RESULT ANALYSIS TABLE

OTP	Website/Tool	Result
ba-Segment-1-1-(-ba-Segment-2-3-*-ba-Segment-6-10-1-ba-Segment-3-15-6-ba-Segment-4-17-8-ba-Segment-5-27-B-	Password Meter	Very Strong
ba-Segment-1-1-(-ba-Segment-2-3-*-ba-Segment-6-10-1-ba-Segment-3-15-6-ba-Segment-4-17-8-ba-Segment-5-27-B-	Password Checker	Excellent Strength
ba-Segment-1-1-(-ba-Segment-2-3-*-ba-Segment-6-10-1-ba-Segment-3-15-6-ba-Segment-4-17-8-ba-Segment-5-27-B-	Cryptool2	Entropy 3.93 Strength 158 Very Strong

V. CONCLUSION

In the modern work , concertation of the data security is must as the lack of security will results in the greater losses whether individual or organizational. Various research has been done to provide or improve the data security. The work which we presented in the dissertation is also the contribution for the same. In the proposed concept, the new approach of picture grid is proposed in which the image segmentation concept is also introduced. The segmented image which placed in the grid will generate the password or OTP pattern with block number combination with the fixed value, this combination with fixed values generates the ASCII value which also concatenated with the pattern. In order to further increase the security, the generated pattern is encrypted using the Hash algorithm with key and then the encrypted OTP is send to the receiver requesting.
In the future, we further like to extend the research in field of video segmentation, audio analysis, and DNA cryptography.

REFERENCES

[1]. Gary Pan, SeowPoh Sun, Calvin Chan and Lim Chu Yeong,"Analytics and Cybersecurity: The shape of things to come",CPA ,2015.
[2]. ErolGelenbe and Omer H. Abdelrahman,"Search in the Universe of Big Networks and Data",IEEE ,2014.
[3]. Benedicto B. Balilo Jr., Bobby D. Gerardo, Ruji P. Medina,"A comparative analysis and review of OTP Grid Authentication Scheme: Development of new scheme",International Journal of Scientific and Research Publications, Volume 7, Issue 11, November 2017
[4]. Anjali Somwanshi,DevikaKarmalkar,SachiAgrawal,PoonamNanaware,Mrs. Geetanjali Sharma, "Dynamic Grid Based Authentication With Improved Security ",International Journal of Advances in Scientific Research and Engineering (ijasre) ,Vol. 03, Issue 3, April -2017
[5]. S. Pandey, R. Motwani, P. Nayyar and C. Bakhtiani, "Multiple access point grid based password scheme for enhanced online security," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 144-148.
[6]. S. Agrawal, A. Z. Ansari and M. S. Umar, "Multimedia graphical grid based text password authentication: For advanced users," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), Hyderabad, 2016, pp. 1-5
[7]. M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), Aligarh, 2017, pp. 171-174
[8]. R. Balaji and V. Roopak, "DPASS — Dynamic password authentication and security system using grid analysis," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 250-253

[9]. E. Yoon and K. Yoo, "Improving the Generalized Password-Based Authenticated Key Agreement Protocol," 2008 The 3rd International Conference on Grid and Pervasive Computing - Workshops, Kunming, 2008, pp. 341-346..

[10]. J.Robinson et al., "Web-enabled grid authentication in a non-Kerberos environment," The 6th IEEE/ACM International Workshop on Grid Computing, 2005., Seattle, WA, USA, 2005