Novel Communication Algorithm with Grid Concept

Manish Kumar Rewadia[1], Shalini[2]

[1]*M.Tech Scholar, Department of Computer Science & Engineering, Jaipur Institute of Technology, Group of Institution, Jaipur, Rajasthan, India*

[2]*Assistant Professor, Department of Computer Science & Engineering, Jaipur Institute of Technology, Group of Institution, Jaipur, Rajasthan , India*

Abstract*:* 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 security the secure file sending is also implemented using the AES encryption and transaction ID concept.

Keywords: *Graphical Password, Grid Authentication, Password security, Security primitives, Secure Communication, Grid Arrangement.*

1. INTRODUCTION

Amid this time when the Internet gives basic correspondence between tremendous quantities of people and is generally speaking dynamically used as a gadget for business, security transforms into a gigantically basic issue to oversee. [1]

There are various edges to security and various applications, stretching out from secure business and portions to private interchanges and guaranteeing passwords. One crucial viewpoint for secure correspondences is that of cryptography, which the point of convergence of this segment is. In any case, it is basic to observe that while cryptography is imperative for secure interchanges, it isn't without any other person's information sufficient. The per client is incited, by then, that the subjects peddled in this part simply depict the first of various crucial for better security in any number of conditions.

During this time when the Internet gives principal communication between a tremendous quantities of people and is generally speaking continuously used as a gadget for business, security transforms into a colossally basic issue to oversee. [2]

There are various points to security and various applications, reaching out from secure business and portions to private communications and guaranteeing passwords. One essential viewpoint for secure communications is that of cryptography, which the point of convergence of this segment is. In any case, it is basic to observe that while cryptography is critical for secure communications, it isn't without any other person's info satisfactory. The per

client is provoked, by then, that the subjects solicited in this part simply depict the first of various essential for better security in any number of conditions.

The Ancient Greek scale (rhymes with Italy), in all probability much like this bleeding edge revamping, may have been one of the soonest devices used to complete a cipher. Before the bleeding edge time, cryptography was concerned solely with message grouping (i.e., encryption) — change of messages from a possible casing into an unfathomable one, and back again at the contrary end, rendering it unclear by interceptors or spies without secret data (specifically, the key required for unraveling of that message). In late decades, the field has stretched out past protection stresses to consolidate techniques for message integrity checking, sender/recipient identity confirmation, automated imprints, wise confirmations, and secure computation, among others. The soonest sorts of riddle forming required negligible more than neighborhood pen and paper relationship, as by far most couldn't scrutinize. More capability, or opponent training, required genuine cryptography[3]. The key conventional cipher forms are transposition ciphers, which reconsider the demand of letters in a message (e.g., 'energize me' pushes toward getting to be 'ehpl em' in an irrelevantly clear adjustment plan), and substitution ciphers, which methodically supplant letters or get-togethers of letters with various letters or social events of letters (e.g., 'fly at once' advances toward getting to be 'gmz bu podf' by supplanting each letter with the one following it in the English letters all together). Essential types of either offered little security from eager enemies, and still don't. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was supplanted by a letter some settled number of positions also down the letters all together. It was named after Julius Caesar who is represented to have used it, with a move of 3, to talk with his officers during his military campaigns, much the equivalent as EXCESS-3 code in Boolean variable based math.

2. LITERATURE REVIEW AND RELATED WORK

E. Yoon and K. Yoo ,2008 [4] Recently, brought up that the upgraded adaptation of the summed up secret phrase based validated key assention protocol proposed by Kwon and Song is insecure against the disconnected secret phrase speculating attacks. Be that as it may, Yeh et al. did not propose an enhanced rendition of Kwon and Song's protocol. Hence, this paper proposes a change of Kwon and Song's improved adaptation that can withstand different crypto graphical attacks and give same proficiency.

J. Robinson, 2005 [5] UABgrid is a coordinated effort among scholarly and managerial IT units at the University of Alabama at Birmingham (UAB). UABgrid gives a Web-based network customer condition, access to shared grounds computational assets, and client personalities characterized by the definitive grounds personality supplier. A Weblogin service utilizing UAB's legitimate character catalog is accommodated lattice authentication. Past mixes of institutional character administration and matrix authentication relied upon a Kerberos domain and utilization of KX.509. We achieve comparable usefulness in a non-Kerberos condition by utilizing our Weblogin service to drive applications which require lattice qualifications. The UABgrid enlistment process utilizes the Weblogin service to produce testaments and keys marked by our UABgridCA and consequently arrangements represents UABgrid clients dependent on asset focus strategies. After effective enrollment, UABgrid use the Weblogin service to enable clients to get to assets and to submit employments utilizing just a Web program and their well-known username and secret word.

P. S. S. Rulers and J. Andrews, 2017 [6] In this paper, we review diverse authentication schemes for graphical passwords used in online services. Snap based graphical secret word scheme is utilized to collect snap focuses or pixel-indicates from clients and forecast the hotspots. CAPTCHA scheme gives security against spyware attacks. On account of Face DCAPTCHA scheme, the clients must perceive outwardly twisted human countenances from complex pictures in a precise way. A Password Guessing Resistant Protocol (PGRP) can restrain vast number of login endeavors from obscure remote hosts to oppose expansive scale online secret word speculating attacks. An Image Recognition CAPTCHA (IRC) called Cortcha is intended to give insurance against machine learning attacks. In the Pass-Go scheme, the client needs to choose PassPoints on a network to include the secret phrase. Formation of cryptographic natives makes the graphical passwords imperceptible to attackers and programmers. A Hotspot or a PassPoint in a picture can be created as a Captcha as gRaphical Passwords (CaRP) picture, or, in other words work, for diminishing security issues happened by online secret phrase speculating attacks, transfer attacks, lexicon attacks and shoulder-surfing attacks.

B. S. Stop, A. J. Choudhury,2011 [7] The rise of present day universal IT, (for example, distributed computing, matrix processing and so on.) builds the utilization of web services. All these web service suppliers utilize client's close to home data, (for example, name, secret word) to verify the client. Moreover, these web service suppliers utilize diverse techniques to secure client's close to home data. Be that as it may, existing security isn't sufficiently secure; noxious attackers may take client entered individual data, for example, clients entered authentication data (ID, Password, declaration number, and so on.) through keyboard snaring. In such manner, this paper proposes a keyboard snaring, SSA, replay attack ensured secret key info technique utilizing authentication example and baffle. The proposed secret word input strategy depends on entering the secret key utilizing mouse. The riddle picture and perplex pixels mapping is haphazardly created.

H. Nicanfar and V. C. M. Leung,2012 [8] In this paper, we consider brilliant framework system requests on remote controlling a shrewd apparatus from up to the focal controller layer, in a private mold and invulnerable from any in the middle of standards' interruption. For example, we have to remotely kill a low-need appeal machine if there should be an occurrence of emergency and crisis, or deal with a module electric vehicles energizing. Subsequently a Home Area Network (HAN) controller ought to be kept from superimposing or contrasting caused by decoding and re-encryption these parcels. Contrasting with X.1035 standard, we utilize just a single hash work and use a crude secret phrase between the apparatus and HAN controller, and state four individual agreement secret phrase validated symmetric key foundations between the machine and upstream controllers during just 12 parcels. We enhance security process data conveyance time by half to 75% while give different attacks flexibility like replay, disconnected speculating, Denning-Sacco, traded off impression, fleeting key bargain impression, obscure key-offer and man in the center.

Qinghai Gao,2012 [9] The Smart Grid being produced across the nation goes for bringing current IT organize into the modern control system (ICS) system to all the more successfully create, transmission, and disseminate power. These systems have their novel vulnerabilities and face a wide range of dangers. Interconnecting them will without a doubt increment many-sided quality, present new vulnerabilities and the joined system will turn out to be more alluring to programmers. How effective the Smart Grid venture can be to a great extent relies upon how well it guards against remote system based attacks. Client authentication for getting to the Smart Grid is the first and most grounded line of resistance against these kinds of attacks. Present day secret word based authentication component has been demonstrated deficient. It is trusted that biometric authentication will

essentially enhance the security of the Smart Grid organize. In this paper we propose utilizing biometrics to confirm clients getting to the Smart Grid. Right off the bat we take a gander at a couple of biometric attributes that have been proposed for client authentication in present day IT arrange and physical access control. At that point we propose security upgraded techniques for applying unique mark for client authentication. The proposed methodologies can help ease client's protection worry for their unique finger impression data, principally because of its customary use for wrongdoing and background examination. Since our strategies enhance the mystery of biometric data, they make it conceivable to incorporate biometrics as a factor in the coveted multifaceted client authentication for the Smart Grid.

S. Sukanya and M. Saravanan, 2017 [10] Nowadays, Banking is a fundamental of human life. Client's informationis put away by the bank. This data is private and sparing securely in the database. Client can process exchanges assignments both on the web and disconnected way. Bank value-based exercises the attacker simple to hack the subtle elements. In this circumstance we need to secure the ledger. Exactly when client input their passwords in an open place, they may be at threat of attackers taking their secret word.

3. PROPOSED WORK

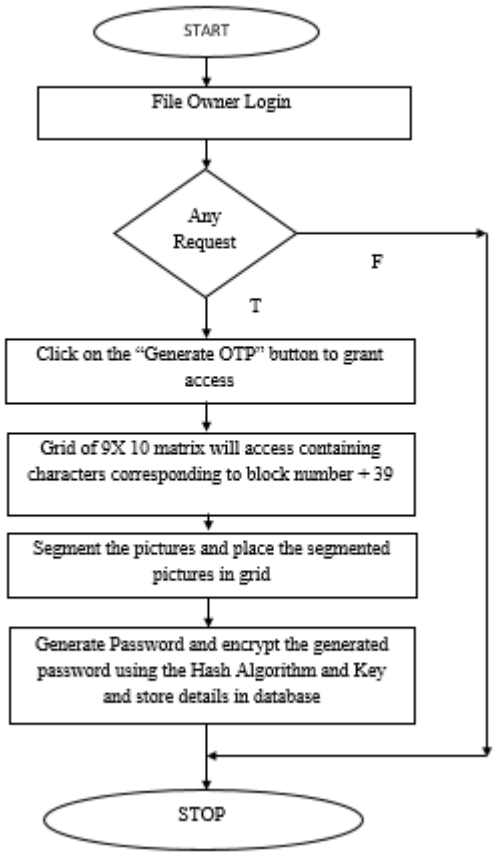

Fig.1 Flowchart for proposed approach

4. RESULT ANALYSIS

We have tried the KEY produced by our proposed usage utilizing the different devices to check its quality. The following is displayed the absolute test investigation introduced on the KEY.

4.1. Password Meter

The webpage www.passwordmeter.com is an online site which tests the quality of the password. This application is expected to assess the quality of password strings. The provoke visual input gives the customer a way to deal with redesign the quality of their passwords, with a hard focus on breaking the customary negative gauges of direct of flawed password ordering. Since no official weighting system exists, they made conditions to diagram the general quality of a given password.

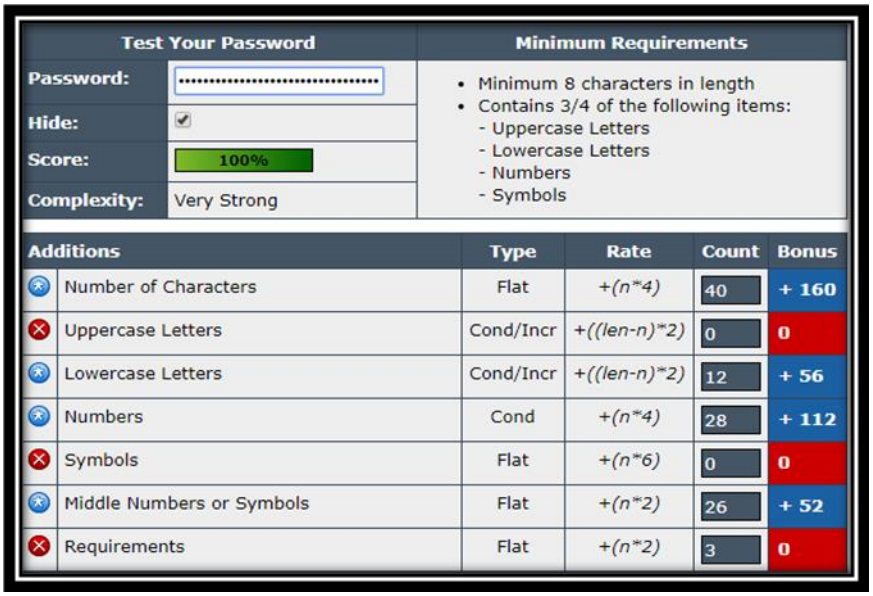

Fig. 2 Test Results for website www.passwordmeter.com

The test password which is given is,

KEY: pe-**Segment-1-1-(-pe-Segment-2-3-*-pe-Segment-6-10-1-pe-Segment-3-15-6-pe-Segment-4-19-9-pe-Segment-5-28-C-**

Result:

Very Strong

4.2 Password Checker

Password Checker Online urges you to assess the quality of your password. Basically more totally, Password Checker online checks the password quality against two fundamental sorts of password breaking systems – the savage propel strike and the word reference assault. It in like manner breaks down the etymological structure of your password and lights up you about its conceivable inadequacies. This instrument can therefore in like manner empower you to make more grounded password from a feeble one.

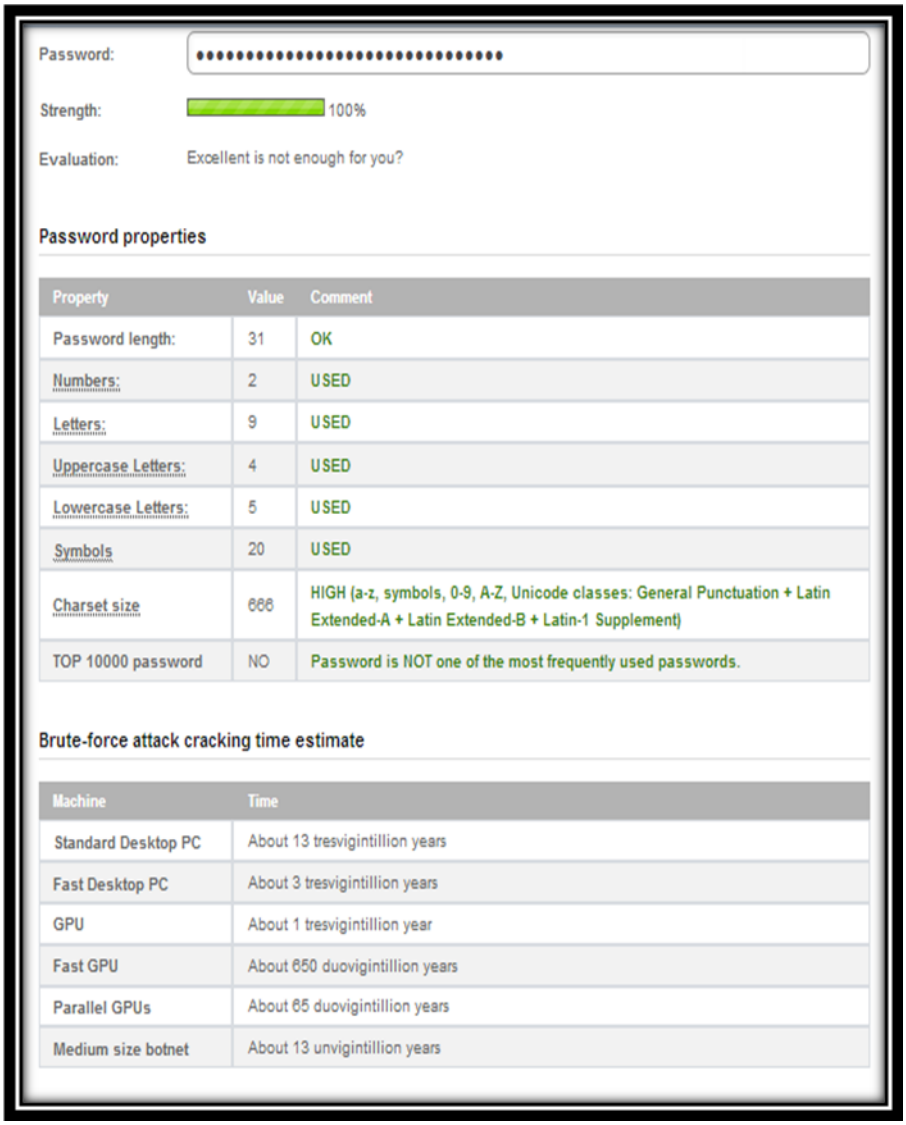

Fig. 3 Test result for OTP online

4.3 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. 4 Test Result using Cryptool2

The Fig. 3 demonstrates the test outcome gotten utilizing the Cryptool2.The above tests can be abridged utilizing the table 1, which demonstrates the consequence of the Key quality utilizing the three instruments which we have taken for the testing reason.

TABLE 1 TEST RESULT ANALYSIS TABLE

OTP	Website/Tool	Result
pe-Segment-1-1-(-pe-Segment-2-3-*-pe-Segment-6-10-1-pe-Segment-3-15-6-pe-Segment-4-19-9-pe-Segment-5-28-C-	Password Meter	Very Strong
pe-Segment-1-1-(-pe-Segment-2-3-*-pe-Segment-6-10-1-pe-Segment-3-15-6-pe-Segment-4-19-9-pe-Segment-5-28-C-	Password Checker	Excellent Strength
pe-Segment-1-1-(-pe-Segment-2-3-*-pe-Segment-6-10-1-pe-Segment-3-15-6-pe-Segment-4-19-9-pe-Segment-5-28-C-	Cryptool2	Entropy 4.93 Strength 198 Very Strong

.

5. CONCLUSION

In the modern work , concentration 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, Seow Poh Sun, Calvin Chan and Lim Chu Yeong, "Analytics and Cybersecurity: The shape of things to come", CPA , 2015.

[2] Erol Gelenbe 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] 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.

[5] 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, pp. 5.

[6] P. S. S. Princes and J. Andrews, "Analysis of various authentication schemes for passwords using images to enhance network security through online services", 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2017, pp. 1-8.

[7] B. S. Park, A. J. Choudhury, T. Y. Kim and H. J. Lee, "A study on password input method using authentication pattern and puzzle", 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, 2011, pp. 698-701.

[8] H. Nicanfar and V. C. M. Leung, "Smart grid multilayer consensus password-authenticated key exchange protocol", 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, 2012, pp. 6716-6720.

[9] Qinghai Gao, "Biometric authentication in Smart Grid", 2012 International Energy and Sustainability Conference (IESC), Farmingdale, NY, 2012, pp. 1-5.

[10] S. Sukanya and M. Saravanan, "Image based password authentication system for banks", 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2017, pp. 1-8.

[11] B. Beckles, A. N. Haidar, S. Zasada and P. V. Coveney, "Audited credential delegation: A sensible approach to grid authentication", 2009 5th IEEE International Conference on E-Science Workshops, Oxford, 2009, pp. 19-30.