Secure Grid based Encrypted File Sharing Algorithm

Komal Sharma[1], Jyoti Choudhary[2], Rahul Sharma[3]
[1]*M.Tech Scholar, Sri Balaji College of Engineering and Technology, Jaipur Rajasthan*
[2,3]*Asst. Professor, Sri Balaji College of Engineering and Technology, Jaipur Rajasthan*

***Abstract*- Security in data communication is very vital. In any type of data transfer, if data is not reached in the proper manner or get manipulated in between before reaching to its receiver, then such communication system is of no use. Seeing the importance and the requirement of the proper and secure communication medium, the proposed work presents the secure communication system which is based on the grid based arrangement of the pictures as well as encryption of the file shared.**

Index Terms- Grid Arrangement, OTP Generation, File Encryption

1. INTRODUCTION

During now once the net offers principal communication between enormous amounts of people and is generally talking unremittingly utilized as a comfort for business, security changes into a hugely fundamental issue to oversee.

There are various focuses to security and various applications, connecting from secure business and parts to non-open communications and ensuring passwords. One basic perspective for secure communications is that of cryptography that the motivation behind union of this stage is. Regardless, it's fundamental to watch that though cryptography is essential for secure communications, it isn't with none extraordinary individual's data tasteful. The per shopper is irate, by at that point, that the themes welcomed amid this half just portray the essential of fluctuated basic for higher security in any scope of conditions. [1]

The Ancient Greek scale (rhymes with Italy), through and through shot exceptionally like this discharge edge patching up, could are one among the most punctual gadgets wont to finish a cipher. Before the drain edge time, cryptography was included just with message gathering (i.e., encryption) revision of messages from a feasible packaging into partner degree inconceivable one, and back yet again at the opposite complete the process of, rendering it hazy by interceptors or spies while not mystery information (explicitly, the key required for unwinding of that message). In late decades, the part has extended past insurance worries to combine procedures for message trustworthiness checking, sender/beneficiary character affirmation, machine-controlled engravings, savvy affirmations, and secure calculation, among others. The soonest assortments of question shaping required immaterial over neighborhood pen and paper relationship, as by a long shot most couldn't investigate. a ton of capacity, or adversary training, required genuine cryptography. The key standard cipher shapes square measure transposition ciphers, that reconsider the interest of letters in an exceedingly message (e.g., 'empower me' pushes toward advancing to be 'ehplem' in partner degree superfluously clear change plan), and substitution ciphers, that systematically override letters or parties of letters with various letters or get-togethers of letters (e.g., 'fly without a moment's delay' propels toward advancing to be 'gmzbupodf' by relocation each letter with the one tailing it inside the English letters all together). Basic sorts of either offered next to no security from enthusiastic foes, and still don't. partner degree early substitution cipher was the Caesar cipher, amid which each letter inside the plaintext was replaced by a letter some settled scope of positions furthermore down the letters at the same time. [3]

2. LITERATURE SURVEY

Anjali Somwanshi et. Al 2017 [4] matter mystery's most ordinarily utilized validation framework for tying down these applications. Verification plots square measure vulnerable against entirely unexpected assortments of attacks. The framework upgrades login security part. The framework incorporates of 6X6 system of twenty six letters so as and ten digits to enter the key expression. though accomplishment inside the framework the shopper

got the chance to give his non-open key which can be utilized while getting into the key expression into the structure. The non-open key of the purchaser can ne'er be utilized anyplace along these lines there aren't any chances of acquiring the key words.

S. Pandey, et. al , 2013 [5] amid this paper, we tend to look at an approach to shield customers' passwords from being taken by adversaries. composed based for the most part mystery state confirmation topic have a bowed to be a great deal of helpless against attacks, for instance, bear aquatics. to defeat the vulnerabilities of standard procedures, visual or graphical mystery key subjects are made as possible elective responses for substance based for the most part conspire. Be that since it could, essentially grasp graphical mystery word verification to boot includes a couple of drawbacks; henceforward some cross breed plans energetic about substance and also styles were made. we tend to propose a virtual mystery state plan just as somewhat live of human procedure to verify customers' passwords in on-line conditions

S. Agrawal, et. al , 2016 [6] Security framework expect an indispensable employment in any framework wherever shopper id includes concern, security frameworks square measure rudimentary for any modernized or propelled get to the executives.

The arranged topic intends to upgrade the steady nature of substance based generally passwords for creative customers by altering a blend of substance and graphical passwords. on these lines a more secure way will be given to customers to allowing access to a checked framework. The arranged idea may be incredibly helpful for ATM machines wherever get to system is by recommends that of an imagine mystery express.

M. H. Zaki ,et .al ,2017 [7] Text-based mystery express verification subject is weakened against different attacks, for instance, bear aquatics attack and practically identical assortment of attacks like word reference attack, savage power attack then on.

Various sensible based generally mystery word confirmation plots square measure there however they're to boot frightfully expensive in causing and wishes a great deal of reaction time at login organize. amid this paper, a more secure precedent key based for the most part mystery express validation subject is arranged which supplies bigger security using blend of model, key, and trick digits. From that time forward, to login, shopper needs to survey the occasion and maps the composed mystery word from precedent with recorded key characteristics, making a mystery expression by just as hoax digits.

It restrains the shoulder aquatics, creature control attacks then on because of high diserse nature of conjecturing mystery express in multilevels: first from model, around then from key and right now from trick characteristics. This subject is run-impervious to basic use issues with the top objective that it doesn't over load human memory and offers further security against obscure attackers.

3. PROPOSED WORK

One Time Password (OTP) is a refined verification subject that offers truth, security and mystery. OTP Two-Factor Authentication is considered mutually of the promising courses in any web-engaged data framework. Starting at now, there square measure different plans are made to guard and verify mystery learning. Regardless, they fluctuate from reasonable properties, ways and materials utilized. the majority of that has outstanding system in dealing with risks and attacks [7]. Lattice validation issue is concerning XY get ready inquiry framework. The impulsive cell inside the lattice passes on the right blend of numbers and letters inside the cell. An instance of matrix verification topic is that the prepackaged game card. it's a less secure decisions as an aftereffects of the 3 digits utilized yet most whimsical OTP plots and may be photocopied making it gave to perils [7].

Regardless, framework confirmation is one among the interesting validation topic that might be explored to flavor up the fanciful time of codes with numerical estimation and algorithmic topic.

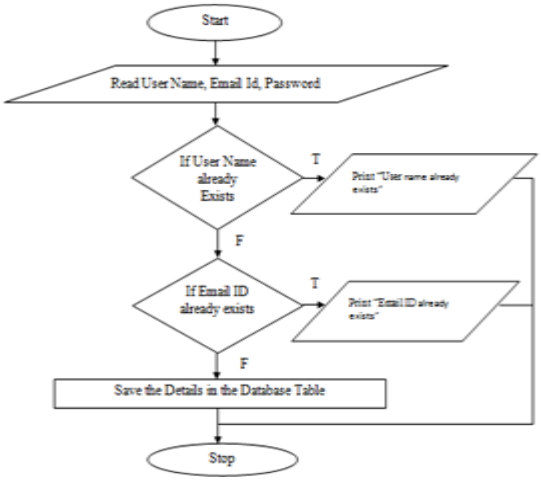

Fig 1 Proposed Concept for Registration.

After the login the next step remains is to share the file and the steps of sending the file and OTP generation are shown in fig 2.

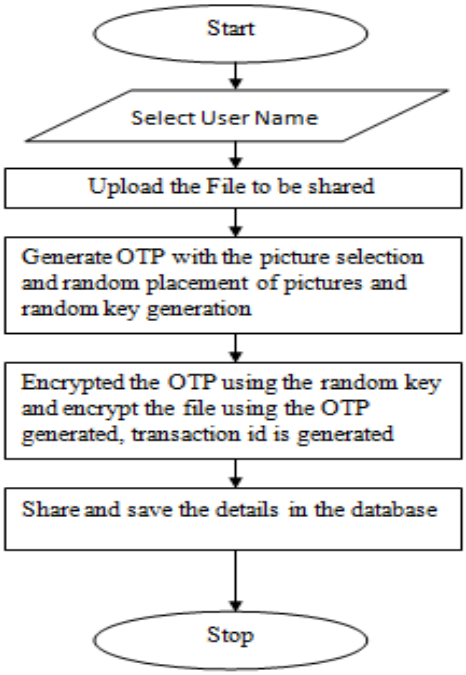

Fig 2. File Sending OTP Generation

After the file is received at the receiver end the following operations are performed as shown in Fig 3.

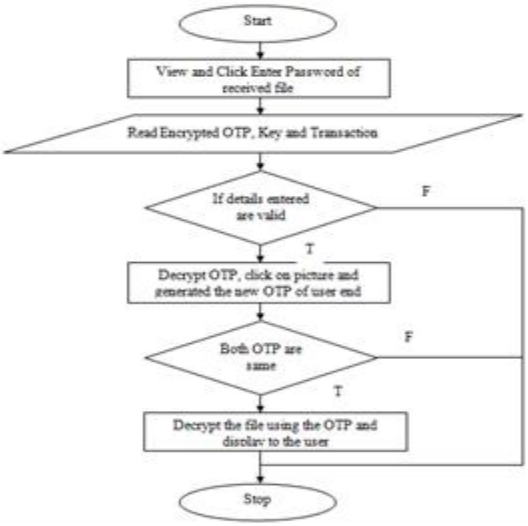

Fig 3. File Receiving

The implementation of the proposed concept is done in the PHP and MYSQL and the implementation snap shot is shown in fig 4.

Fig 4. OTP generation in PHP

4. RESULT ANALYSIS

The OTP generated is tested using the various tools and software's which are used for the cryptanalysis and the result is shown in table 1.

Table 1. Result Comparison

Base Work	OTP	Website/Tool	Result
TWE	ph-Segment-3-43-R-ph-Segment-5-4-+-ph-Segment-6-77-t-ph-Segment-2-75-r-ph-Segment-1-33-H-ph-Segment-4-58-a-	Password Meter	Base : 5% Proposed : 100% Very Strong
TWE	ph-Segment-3-43-R-ph-Segment-5-4-+-ph-Segment-6-77-t-ph-Segment-2-75-r-ph-Segment-1-33-H-ph-Segment-4-58-a-	Password Checker	Base : 4% Proposed : 100% Very Strong
TWE	ph-Segment-3-43-R-ph-Segment-5-4-+-ph-Segment-6-77-t-ph-Segment-2-75-r-ph-Segment-1-33-H-ph-Segment-4-58-a-	Cryptool2	Base : Strength 60 ,Entropy :2.23 Entropy 3.68 Strength 102 Very Strong

5. CONCLUSION

The proposed work presents the secure communication system which is based on the grid based arrangement of the pictures as well as encryption of the file shared. The proposed system let the user to select any file , whether the text , video or any other type of file and generate the OTP for file sharing on the basis of the random placement of the segmented pictures in the grid. The randomly generated key will be used for the encryption of the OTP and the OTP itself is used for the encryption of the file uploaded and shared. The reverse mechanism of the decryption of the OTP and file shared is performed at the receiver end. The result obtained on comparison of the OTP generated is made with the previous work done and the result are quite effective and impressive.

REFERENCES

[1] Puneet Singh Duggal, Sanchita Paul "Big Data Analysis: Challenges and Solutions" International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV.

[2] Zan Mo, Yanfei Li "Research of Big Data Based on the Views of Technology and Application" American Journal of Industrial and Business Management, 2015, 5, 192-197.

[3] K.Arun, Dr.L.Jabasheela "Big Data: Review, Classification and Analysis Survey" International Journal of Innovative Research in Information Security (IJIRIS) Volume 1 (September 2014) ISSN: 2349-7017(O) ,ISSN: 2349-7009(P)

[4] Anjali Somwanshi,Devika Karmalkar,Sachi Agrawal,Poonam Nanaware,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] Kalyani Shirudkar, Dilip Motwani "Big-Data Security" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 3, March 2015.

[9] Nishu Arora, Rajesh Kumar Bawa "A Review on Cloud to Handle and Process Big Data" International Journal of Innovations & Advancement in Computer Science IJ IACS ISSN 2347 – 8616 Volume 3, Issue 5 July 2014

[10] A B M Moniruzzaman, Syed Akhter Hossain "NoSQL Database: New Era of Databases for Big data Analytics-Classification, Characteristics and Comparison" International Journal of Database Theory and Application Vol. 6, No. 4, August, 2013.Shilpa, Manjit Kaur "BIG Data and Methodology-A review" Volume 3, Issue 10, October 2013.

[11] P. V. Maitri, D. S. Waghole and V. S. Deshpande, "Low latency for file encryption and decryption using BRA algorithm in network security," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-4.

[12] S. Wang and G. Liu, "File Encryption and Decryption System Based on RSA Algorithm," 2011 International Conference on Computational and Information Sciences, Chengdu, China, 2011, pp. 797-800.doi: 10.1109/ICCIS.2011.150.