Dual Verification Scheme Using Transaction ID and Random Key

[1]Rajeshkumar P.Dave, [2]Yashwant Soni
[1]PG Scholar, [2]Assistant Professor
[1] Shobhasaria Engineering College. Sikar(Rajasthan) (India)
[2] Shobhasaria Engineering College, Sikar(Rajasthan) (India)

Maintaining the security during the data transfer is the foremost requirement of the data communication. Security is the main concern in the transaction, the proposed dissertation has increased the security first by making use of the variable length captcha to be used as the OTP for sharing and accessing the file. As the length of the OTP is variable as its selected on random and also include the random characters, so the unpredictability of password or OTP makes it more secure. In this paper, for the same, we present the secure data communication concept by making use of the unique transaction id and the dynamic random password concept.

Keywords: Secure data communication, transaction id, dynamic password

I. INTRODUCTION

The procedure for demonstrating one's manner. It's another piece of data security that we watch out for fitness with customary workstation utilization. Simply expect once you sign into your email, or diary account. The key sign-in method may be a sort of check that stipends you to sign into applications, records, organizers and even a full workstation structure. [1] Once set apart in, you have exceptionally astounding given edges till the reason once works out. Some structure can wipe out a session if your machine has been sit still for an explicit live of your chance, requiring that you essentially indicate validation at the most astounding purpose of the day to get in. The fundamental sign-on think up is to boot existent into solid client affirmation frameworks. Be that since it might, it envisions that people will login utilizing vacillated [2] parts of validation. Non-repudiation: in the midst of this, the recipient should catch paying little heed to whether the sender isn't faking. for example, if acknowledge once one makes one thing on the net, one must be compelled to watch that that the individual whom one pays isn't faking. Reliability: usually data ought to be invigorated regardless this should be finished by significant people. Security/grouping: confirming that no one will check the message aside from the masterminded gatherer.

Encryption [3] is that the system for clouding data to make it uncertain while not specific learning. Encoding has been used to stay exchanges for an impressive length of your chance, yet just affiliations a people with an exceptional interest for riddle had made utilization of it. inside the mid-1970s, in run encoding up out of the principle extra of secured government relationship into the last people house, and is eventually used as a locale of making certain roughly used frameworks, for example, Web on-line business, cell phone frameworks and bank adjusted teller machines. encoding may be used to ensure question, anyway exceptionally astonishing frameworks zone unit so far foreseen that would make correspondences secure, particularly to envision the decency and legality of a message, for example, a message validation code (MAC) or pushed marks.

Another considering is confirmation against activity examination. Impedance may be dealt with by causation a flag to the beneficiary, the one that sends the affirmation development back to the transmitter, the data will be sent just to it gatherer. In the midst of thusly with the use of insistence signals obstruction may be sidestep. A block-based image encryption algorithm using a chaotic permutation. Experiment shows that the cipher-images that resulted from the algorithm are robust to common image processing operations. Such image processing are JPEG compression, image noising, and image resizing. The decrypted images can be still recognized well, although they are just like noised.[4].

II. Related Work

Iqbal, Saima and Lal Yadav, Ram [5] As there is tremendous addition or rise in the data exchange by the electronic system, the requirements of data security have transformed into a motivation. The most basic stress in the communication system which is among sender and gatherer is the security of the data which is to be transmitted. To discard the intruders, diverse cryptographic estimations are used for example, AES, DES, Triple DES, Blowfish, etc. In this paper, makers have tried to trade report securely using erratically delivered keys with Blowfish symmetric estimation for encryption process. A stand-out trade id is in like manner delivered which is used to get the unpredictable key which will be used for unscrambling at the recipient end. A validation key is similarly proposed which is used to affirm that archive is unscrambled by the arranged customer figuratively speaking. The blend of of unpredictable key, validation key, and trade id as proposed will give more life to secure trade of report using Blowfish symmetric key encryption.

A. Agarwal and S. J. Singh [6] This paper speaks to the use of pre-flowed data/procedures for mystery key assignment with the help of Encode-Decode IDs(IDentifications) and limits (used for creating yield reliant on nonce). Moreover, certain attacks recorded in composing on various traditions has in like manner been thought close by giving included strike revelation feature achieved due to these Masked IDs. The arrangement analyzed has an extra favored point of view of diminishing number of trades/steps required in attack acknowledgment.

C. Carreto, M. A. Diaz and B. Carvajal [7] In this paper the headway of a Standard Model and Architecture of Digital ID (MAEID) is seemed to enable security parts, which enable the unmistakable verification and confirmation to secure trades in an educational circumstance. These ontologies based instruments (data structure), open key cryptography (encryption, propelled assertions, modernized imprints, etc..) And biometrics, executed truly meeting the most basic security essentials for the unambiguous unmistakable proof of its proprietor and procure the piece of tying down the organizations and who is required appraisals favor. An examination of the developments included are furthermore presented, the issues which may defy who need to execute this model, proposals and possible alternatives as opposed to the progression of a structure for conspicuous evidence and verification.

Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen and L. Tooth [8] Authenticated key Exchange (AKE) tradition empowers a customer and a server to approve each other and make a session key for the subsequent communications. With the quick enhancement of low-control and exceptionally viable frameworks, for instance, unavoidable and adaptable figuring framework starting late, various gainful AKE traditions have been proposed to achieve customer security and validation in the communications. Other than secure session key establishment, those AKE traditions offer some other supportive functionalities, for instance, two-factor customer validation and shared confirmation. In any case, most of them have something like one deficiencies, for instance, shortcoming against lost-shrewd card attack, separated word reference ambush, de-synchronization strike, or the nonattendance of forward puzzle, and customer mystery or untraceability. Additionally, an AKE contrive under the all inclusive community key structure may not be sensible for light-weight computational contraptions, and the security model of AKE does not get customer indefinite quality and contradict lost-sharp card ambush. In this paper, we propose a novel exceptional ID-based obscure two-factor AKE tradition, which keeps an eye on all the above issues. Our tradition moreover supports sharp card renouncement and mystery word invigorate without concentrated limit. Further, we extend the security model of AKE to help customer anonymity and restrict lost-sharp card ambush, and the proposed arrangement is provably secure in widened security appear. The low-computational and exchange speed cost demonstrates that our tradition can be passed on for certain enlisting applications and adaptable communications eventually.

K. Lin, L. Yuan and G. Qu [9] Data extortion and Mastercard trickery are among the genuine security issues for online shopping and diverse trades. Current industry standard of multi-point singular data amassing does not secure customer's identity suitably. Various online shipper servers use mystery state verification technique, whose security defects have been particularly recorded. In spite of the way that there are various troubles in achieving secure online trade, we propose a structure that can essentially reduce the threat of discount extortion over the Internet by engaging customers to disguise their characters from the online merchants and, to some expand, the Internet. Our system configuration diminishes the above multi-point data accumulating structure to a single point separated course of action. That is, customer's near and dear data will be secured on a secure disengaged database and a gave USB contraption. Such data won't be sent to the merchants to complete the online trades. The SecureGo device can be related with any host PC for online trades, anyway unscrambling and encryption will be performed locally on the SecureGo USB device to deflect ambushes, for instance, the dangerous host. This is an authentic hardware programming co-protection approach to manage ensure secure online trades and customer's assurance. The dedicated hardware, the USB contraption, completes the secure (programming) errands and has an extraordinary ID to cover the customer's character.

H. Al Housani, Joonsang Baek and Chan Yeob Yeun [10] In the prospect of regular open key system (PKI), we need to pass on open keys truely. Even more unequivocally, electronic confirmation ties an open key with the identity of its proprietor. Regardless, vital overhead is connected with supervising mechanized supports. Henceforth, the new thought called "character based open key cryptography" (ID-PKC) in which bitstring of customer identity (could be name, email addresses, etc) is direct being the overall public key. The private key generator (PKG) is accountable for making customers private keys according to their open keys (characters). In this way, the need of validations is abstained from in light of the way that the authenticity of individuals when all is said in done key is extremely cultivated. Of course, key escrow issue exists since PKG can find (discover) any customer's private key. Okay have the capacity to imagine what a harmful or dealt PKG can do? With the ultimate objective to beat this issue another perspective which is certificateless open key cryptography (CL-PKC) is displayed in which the private key is for the most part managed by the key creating center (KGC). In this paper we analyze the key CL-PKC plot which is proposed by Al-Riyami and Paterson.

H. Wang, D. He and S. Tang [11] A regularly expanding number of clients should need to store their data to open cloud servers (PCSs) close by the quick enhancement of dispersed figuring. New security issues must be comprehended with the ultimate objective to empower more clients to process their data out in the open cloud. Exactly when the client is constrained to get to PCS, he will assign its mediator to process his data and exchange them. On the other hand, remote data integrity checking is moreover a basic security issue out in the open dispersed capacity. It makes the clients check whether their redistributed data are kept faultless without downloading the whole data. From the security issues, we propose a novel delegate arranged data exchanging and remote data integrity checking model in character based open key cryptography: identity based mediator organized data exchanging and remote data integrity checking without trying to hide cloud (ID-PUIC). We give the formal definition, system model, and security show. By then, a strong ID-PUIC tradition is organized using the bilinear pairings. The proposed ID-PUIC tradition is provably secure subject to the hardness of computational Diffie-Hellman issue. Our ID-PUIC tradition is furthermore capable and versatile.

In perspective of the principal client's endorsement, the proposed ID-PUIC tradition can comprehend private remote data integrity checking, delegated remote data integrity checking, and open remote data integrity checking.

M. Sarvabhatla and C. S. Vorugunti [12] As frameworks organization and remote communication progresses advance even more rapidly, it offer climb to a smart change in the m-exchange arrive scape. The insecure open internet as a passageway medium realized groups of cryptographic attacks on remote trades. Along these lines, there is a phenomenal enthusiasm for light weight and secure confirmation traditions. In this one of a kind circumstance, couple of researchers have proposed E.C.C based validation intends to affirm the realness of the customer interfacing with remote server. Starting late Islam et al has proposed a dynamic ID based verification plot using E.C.C and ensured that their arrangement is secure and versatile. In this unique duplicate, we will demonstrate that their arrangement is defenseless to detached mystery state conjecturing attack and customer emulate strike. We by then pass on a secure and ground-breaking validation plot, which is impenetrable to each and every cryptographic ambush and light weight. We have dismembered security characteristics of our arrangement formally using discretionary prophet model and redirection theory.

Z. Gao, S. H. S. Huang and W. Ding [13] Remote customer verification is an instrument in which the remote server affirms the validness of a customer over an open and insecure communication channel. Mystery express confirmation using a splendid card has been one of the routinely grasped procedures to guarantee the mystery word during transmission. Starting late, various masters have proposed a movement of dynamic ID-based remote customer validation designs with the component that the customer's identity is changed in each trade session.

III. Proposed Work

In the proposed work, we have first used the random key for the key which is used in the blowfish encryption and decryption process and the algorithm for the random key generation is process is

Algorithm for Random Key Generation

```
Step 1: Initialize an array KeyChar with the hexadecimal values such that, KeyChar[1]='a' , KeyChar[2]='b' and so on KeyChar[16]='9'.
Step 2: Repeat Step 3 to for I : = 1 to 64 do
Step 3: Set index : = Rand(1:16). Step 4: Set s := s +KeyChar[index].
[End of for loop]
```

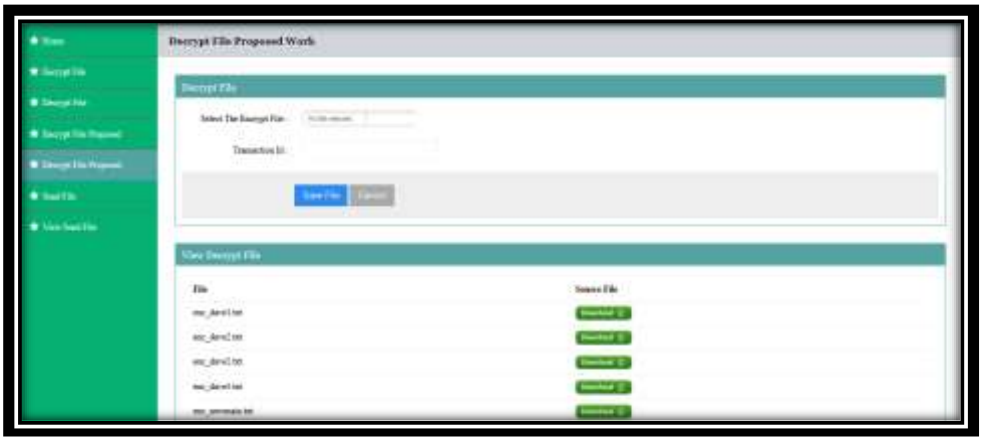
Now s will contain the random key generated via the above mentioned algorithm. In the proposed concept we have created the following Framework for the message transferring from the sender and receiver using the modified blowfish algorithm.

Algorithm for Generating the Transfer Key

```
Step 1: Access the Name of Sender and Receiver.
Step 2: Calculate the length of sender username.
Step 3: Calculate the length of receiver username.
Step 4: Encrypt all characters of the sender user name by adding up the length of sender username in the characters corresponding to the sender username.
Step 5: Encrypt all characters of the receiver user name by adding up the length of receiver username in the characters corresponding to the receiver username.
Step 6: Concatenate the string patterns obtained from the step 4 and step 5 and the resultant pattern is the TRANSFER KEY.
```

Algorithm for Generating Random OTP

```
Step 1: Random length for the OTP is selected , which means that the length of the OTP may vary time to time and store the generated .
Step2 : Set I=1 ,S="". [ where S is the string which will contain the generated password]
Step 3: Repeat Step 4 to7 while I<=N do:
Step 4: Set K :=Random(Length of Array Containing Characters)
Step 5: Set Ch :=(char)K [Convert the number into character]
Step 6: Set S:=S+Ch.
Step 7: Set I:=I+1.
    [End of while Loop]
Step 8 : Then mail the generated pin to the user and user then re-enter the pin in the space provided.
```



Decrypt File Proposed Work

Decrypt File

Select The Encrypt File:

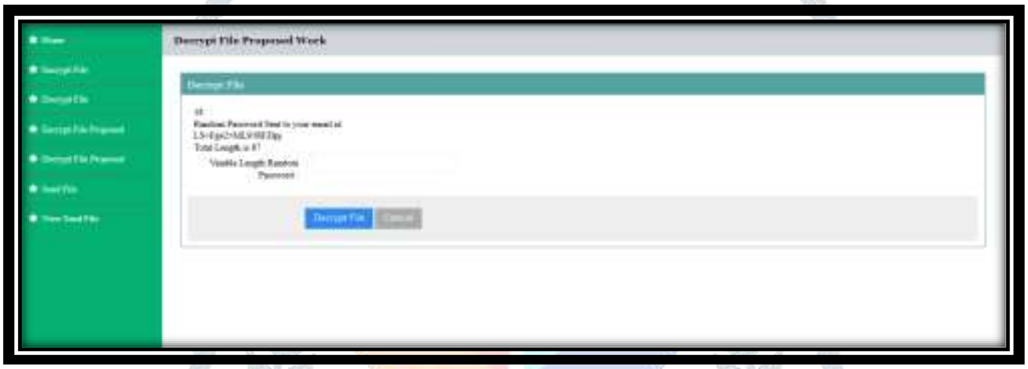
Transaction Id:

View Decrypt File

File	Source File
[illegible]	Download
[illegible]	Download
[illegible]	Download
[illegible]	Download
[illegible]	Download

Fig 1. Implementation for Transaction ID

The implmenentation of the proposed work is done in PHP and MYSQL and the concept of using the dynamic ramdom key as the receiver end valudation is show in Fig 2.



Decrypt File Proposed Work

Decrypt File

[illegible]
Random Password Send to your email id
[illegible]
Total Length is [illegible]
Variable Length Random Password

Fig 2. Dynamic Password Receiver End

IV. Result Analysis

The result analysis is done by comparing the key using the various websites like password meter , password checker and also the tool cryptotool2 . The result obtained is shown in the table 1.

Test KEY	Website/Tool	Result
��- Go5����6����O�����O�� ���z	Password Meter	Very Strong
��- Go5����6����O�����O�� ���z	Password Checker	Excellent Strength
��- Go5����6����O�����O�� ���z	Cryptool2	Entropy 3.825 Strength 129 Very Strong

V. Conclusion

Security is the main concern in the transaction; the proposed dissertation has increased the security first by making use of the variable length captcha to be used as the OTP for sharing and accessing the file. As the length of the OTP is variable as its selected on random and also include the random characters, so the unpredictability of password or OTP makes it more secure.

Thus, we can say that our proposed implementation provides a better way to share the data securely.

Together with the green concept in the dissertation, our work also focus on the security, by making the use of the Random password together with the transaction id, we have enhance the security, thus overcoming the probability of the easily cracked passwords.

Future Work: In the future work we will try to extend our research towards the search of the images and other complex data and in segment of security we will try to extend our work with the DNA Passwords, ECG cryptography and similar concepts.

REFERENCES

[1]. Deepika, Manpreet," A Review on Various Key Management Techniques for Security Enhancement in WSN",International Journal of Engineering Trends and Technology (IJETT) – Volume 34 Number 4- April 2016.

[2]. Vaibhav Poonia , Dr. Narendra Singh Yadav ,"Analysis of modified Blowfish Algorithm in different cases with various parameters" ,International Journal of Engineering Research and General Science 2015.

[3]. Md. Asif Mushtaque and Hash Dhiman "Implementation of New Encryption Algorithm with Random Key Selection and Minimum Space Complexity", International Conference on Advances in Computer Engineering and Applications (ICACEA) ,2015.

[4]. Deepak Kumar Singh, Kuldeep Tomar: A Robust Color Image Encryption Algorithm in Dual Domain using Chaotic Map, 2nd International conference on Inventive Communication and Computational Technologies (IEEE 2018)

[5]. Iqbal, Saima & Lal Yadav, Ram, A Secure File Transfer Using the Concept of Dynamic Random Key, Transaction Id and Validation Key with Symmetric Key Encryption Algorithm,Proceedings of First International Conference on Smart System, Innovations and Computing (2018), 2018

[6]. A. Agarwal and S. J. Singh, "Mask IDs based asymmetric session key exchange," 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), Chirala, 2017, pp. 418-422.

[7]. C. Carreto, M. A. Diaz and B. Carvajal, "Developing an implementation model and Architecture Standard Digital ID," 2016 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, 2016, pp. 1-6.

[8]. Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen and L. Fang, "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol With Extended Security Model," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382-1392, June 2017.

[9]. K. Lin, L. Yuan and G. Qu, "SecureGo: A Hardware-Software Co-Protection against Identity Theft in Online Transaction," 2007 ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security (BLISS 2007), Edinburgh, 2007, pp. 59-64.

[10]. H. Al Housani, Joonsang Baek and Chan Yeob Yeun, "Survey on certificateless public key cryptography," 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 53-58.

[11]. H. Wang, D. He and S. Tang, "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165-1176, June 2016.

[12]. M. Sarvabhatla and C. S. Vorugunti, "A secure and robust dynamic ID-based mutual authentication scheme with smart card using elliptic curve cryptography," 2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), Bengaluru, 2015, pp. 75-79..