International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557 Volume-5, Issue-6, November 2018
www.ijirem.org

Secure Data Storage Using Hybrid Cryptography

Vijaypal Singh
Department of computer science & Engg, G L Bajaj Institute of Technology & Management,
Gr Noida, India

Sunny Chauhan
Department of computer science & Engg, G L Bajaj Institute of Technology & Management,
Gr Noida, India

Markandey Tiwari
Department of computer science & Engg, G L Bajaj Institute of Technology & Management,
Gr Noida, India

Jai Vikrant
Department of computer science & Engg,
G L Bajaj Institute of Technology & Management,
Gr Noida, India

ABSTRACT

To protect our data from being misused we need to secure our information. To secure data there are various encryption algorithms available. In this we Divide our data in 3 parts and encrypt the data using 3 Different encryption algorithms . After this a key is generated which is used as a secret key for decryption. The Cipher Text and Key is given to the recipient through which they can decrypt the message.

Keywords

Encryption, Decryption, cipher Text, secret Key, Cryptography

1. INTRODUCTION

In this paper we secure a text transmitted over the internet using Hybrid Cryptography. In Hybrid Cryptography we use 3 different types of algorithm .ie. AES , DES and RC2 for encrypting our text .

In cryptography, the path toward encoding a message or information with the goal that singular endorsed social affairs can get to it and the people who are not affirmed can't is known as Encryption. Encryption don't balance impedance itself, anyway denies the conceivable substance to a future interceptor. In an encryption, the proposed information or message, which is insinuated as plaintext, is encoded by using an encryption computation – a figure – delivering figure message that can be scrutinized just at whatever point unscrambled. For specific reasons, an encryption count generally uses a pseudo-unpredictable encryption key made by a computation. It is on a crucial dimension possible to unscramble the message without having the key, yet, for a well-organized encoded structure, huge computational resources and capacities are required. An affirmed recipient can without a doubt disentangle the message with the help of key given by the originator to recipients yet not to a customer who is unapproved. Militaries and governments use encryption to energize their riddle correspondence. It is by and by a day's generally used in guaranteeing information inside various sorts of non-military work force systems. For example, The PC Security Foundation had reported that in 2007, 71% of associations had utilized encryption for a part of their data that they use, and 53% utilized encryption for a segment of their data they have secured. Encryption can be used to guarantee data which is "still, for instance, information that are secured on PCs and limit devices (for instance USB streak drives). In the midst of progressing years, there have been enormous number of reports of mystery data, for instance, a customers' near and dear records, being revealed through adversity or burglary of PCs or fortification drives; encryption of such archives still guarantees them if physical wellbeing endeavors disregard to verify. Propelled rights the officials systems, which turns away unapproved usage or augmentation of copyrighted materials and data and guarantee programming against making sense of, is another particular instance of using encryption on data extremely still.

A hybrid Cryptography scheme is the one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme.

Half breed encryption is made possible through data trade using exceptional session keys close by symmetrical encryption. Open key encryption is completed for self-assertive symmetric key encryption. The open key encryption technique is used by the recipient to unscramble the symmetric key. At the point when the symmetric key is recovered, by then it is used to disentangle the message.

The blend of encryption methods has various focal points. One is that an affiliation channel is developed between two customers' courses of action of apparatus. Various Clients by then get the opportunity to grant through cross breed encryption. Uneven encryption can ceaselessly frustrate the encryption method, anyway with the execution of synchronous use of symmetric encryption, the two kinds of encryption plans are updated. The result is then included security of the transmittal method close by overall improved execution of the framework.

2. OBJECTIVE AND SCOPE

The Objective of the paper is to secure our data using Hybrid Cryptography . In Present there are various systems present for transferring of data over the internet. Most of them used a single encryption algorithm for securing our data .

3. METHODOLOGY

For Encryption we have used 3 Encryption Algorithms .i.e.

- AES (Advanced Encryption System)
- DES (Data Encryption Standard)
- RC2

3.1 For Encryption

- The user Logs in the web application using various provided credentials.
- Users types the message on the text box which is to be sent 3. The encrypted text is generated along with key.

3.2 For Decryption

- The user Logs in the web application using various provided credentials.
- User enters the encrypted text and key in the mentioned fields.
- Original message is generated.

4. RESULTS & DISCUSSION

The text generated after Encryption is known as Cipher Text and is completely different from the Original Text. While Data Transfer only Cipher Text is given to the recipient.

Decrypted String - Encryption, independent from anyone, can ensure privacy of messages, yet various different methods are as yet expected to secure the honesty and legitimacy of a message; for instance, check of a message verification code (Macintosh) or a computerized mark. Benchmarks for the cryptographic programming and equipment to perform encryption are generally accessible, yet effectively utilizing encryption to guarantee security might be a difficult issue. A solitary blunder in framework plan or execution can permit effective assaults. Now and again a foe can get decoded data without legitimately fixing the encryption. It's just obvious, e.g., traffic investigation, Storm, or Trojan pony

5. DECRYPTION

Decrypted String - Encryption, independent from anyone, can ensure privacy of messages, yet various different methods are as yet expected to secure the honesty and legitimacy of a message; for instance, check of a message verification code (Macintosh) or a computerized mark. Benchmarks for the cryptographic programming and equipment to perform encryption are generally accessible, yet effectively utilizing encryption to guarantee security might be a difficult issue. A solitary blunder in framework plan or execution can permit effective assaults. Now and again a foe can get decoded data without legitimately fixing the encryption. It's just obvious, e.g., traffic investigation, Storm, or Trojan pony

6. CONCLUSION

It is almost impossible to decrypt the message without the help of key. Thus, this can be used by various messaging applications and all email providers to secure their messages. This technique can be used to transfer messages securely across all platforms over the internet.

Utilizing just a solitary encryption calculation renders it defenseless against numerous assaults that assault the feeble chinks in the calculation's love particularly most calculations face grave risk against beast power assaults. In this way by utilizing numerous calculations in a succession where the yield of one calculation is the contribution for the following calculation in the arrangement gives additional security by verifying the information exponentially well and the adaptability of the system as referenced before makes it magnificent to be utilized with future calculations and furthermore to be executed with passwords for additional insurance. The numerous encryption calculations utilized alongside the haphazardness in nature of the determination of the calculations, their succession and the quantity of calculations utilized gives a great deal of security in different layered way when contrasted with the calculations utilized as an independent substances and gatekeepers against some outstanding assaults.

REFERENCES

[1] http://www.crypto-it.net/eng/symmetric/des.html?tab=2

[2] https://ieeexplore.ieee.org/abstract/document/5437735

[3] Matt Pharr, Randima Fernando, "GPU Gems 2: Programming Techniques for High-Performance Graphics and General-Purpose Computation" in , Addison-Wesley Professional, 03 2005.

[4] https://ieeexplore.ieee.org/document/563518 M. E. Hellman, "DES will be totally insecure within ten years", IEEE Spectrum, vol. 16, no. 7, pp. 32-39, July 1979.

[5]https://www.researchgate.net/publication/228952571_RC2_Encryption_and_Decryption_in_Microsoft_NET

[6] https://www.geeksforgeeks.org/computer-network-data-encryption-standard-des-set-1/