Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Technique to Enhance Network Security Using TDES and MD5 in OTP

Pushpanjali Pandey
Department of Computer Science & Engg.
Uttarakhand Technical University
Dehradun, India

Dr. B.M Singh
(Associate Prof.)
Head of Department of IT
COER Roorkee, India

Abstract— Today's dynamic and data rich environment, data frameworks have ended up crucial for any organization to survive. With the raise in the reliance of the organization on the information system, there exists chance for the competitive organizations and disrupting forces to achieve access to other organizations information system. This unreceptive environment makes information systems security problem crucial to an organization. Hence the best ways to provide security is Cryptography and Steganography. Cryptography and Steganography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood and produces a cipher text. The information security is one of the critical problems in data communication. So it becomes an integrated part of data communication. Hence for addressing this issue, cryptography and steganography can be merged. This paper proposes a secure communication system.

Index Terms—Component, formatting, style, styling, insert. (key words)

I. INTRODUCTION

Cryptography: - Cryptography is the practice and study of hiding information. In today's environment, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in technologically advanced applications, including areas such as the security of ATM cards, PC passwords, and electronic commerce which all rely on upon cryptography. Cryptography has long been of interest to intelligence gathering and law enforcement agencies. Modern cryptography, necessary to the security of PC systems, is finished with complex calculations executed on rapid PC frameworks. Normally saying computer cryptographic tasks can be classified in two broad categories: encryption and authentication [1].

Cryptographic algorithms are catertogied as symmetric key algorithm and public key algorithm. Symmetric key algorithm utilizes the same key for encryption and decryption, while public key algorithm uses different keys for encryption and decryption. Steganography system can be implemented via two techniques. Firstly, the spatial domain based steganography, where the least significant bits (LSB) of the cover object is replaced by the secret message bits. Secondly, the transform domain based steganography; in this case, the secret message is embedded with the coefficient of the cover object. The most common transform domains are discrete Fourier transform and discrete wavelet transform.

To improve the reliability of the communication system; the two can be merged to implement a robust and secure system; in this case, the encryption and hiding are achieved in the transmitter, while the extraction and decryption are achieved in the receiver. [2].

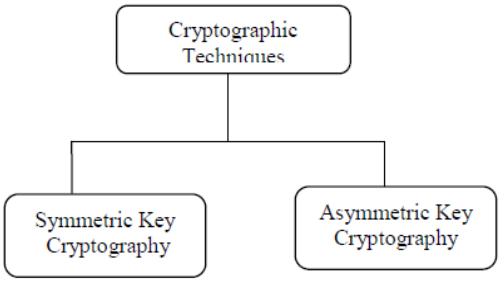

Figure 1 Cryptography Technique

Encryption refers to the scrambling of data so that the original data is difficult to be discovered by unauthorized receiver. An encryption algorithm is applied to the data, known as plaintext, and a *key* to generate cipher text, which preferably appears to be random bits.

A decryption algorithm transforms the cipher text back into plaintext, but having the accurate key. Conventional, or symmetric, algorithms utilize the same key for both encryption and decryption. Public key algorithms use paired keys, one for encryption and another for decryption.

II. CRYPTOGRAPHY ALGORITHM

Triple Data Encryption Standard (TDES):

3DES

3DES (Triple DES) is an improvement of DES; it is a 64 bit piece size through 192 bits key size. In this standard the strategy for encryption is same to the one in the first DES yet connected 3 times to development the encryption level furthermore the normal safe time. 3DES is slower than other distinctive piece figure approaches. It utilizes either a few diverse 56 bit keys in the succession EDE (Encrypt-Decrypt-Encrypt). Essentially, three different keys are utilized for the encryption calculation to make figure content on plain instant message, t.

$C(t) = Ek1(Dk2(Ek3(t)))$ (1)

Where C(t) is cipher text produced from plain text t,
Ek1 is the encryption method using key k1
Dk2 is the decryption method using key k2
Ek3 is the encryption method using key k3

Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$C(t) = Ek1(Dk2(Ek3(t)))$ (2)

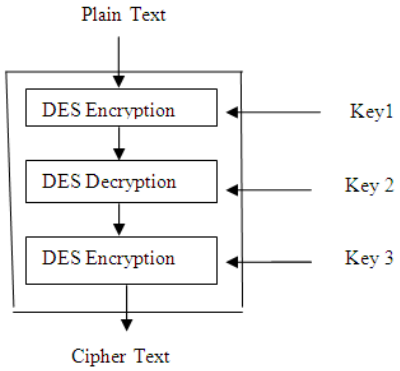

Figure: Encryption in 3DES

algorithm of TDES with the three different keys need 2^168 probable combinations and also two different keys need 2^112 combinations. It is essentially not possible to try such a large combination so TDES is a algorithm of strongest encryption. The algorithm drawback it is too time consuming.

MD5:

MD5 [4] is an algorithm that is utilized to check information through the making of a 128-bit message digest from information data (which may be a message of any length) that is guaranteed to be as one of a kind to that particular information as a unique fingerprint is to the particular person. MD5, which was produced by Professor Ronald L. Rivest of MIT, is proposed for utilization with digital signature applications, which require that substantial documents must be compacted by a safe system before being encoded with a secret key, under a public key cryptosystem. MD5 is as of now a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. As indicated by the standard, it is "computationally infeasible" that any two messages that have been information to the MD5 algorithm could have as the yield the same message digest, or that a false message could be made through worry of the message digest. MD5 is the third message digest algorithm made by Rivest. All three (the others are MD2 and MD4) have similar Each of the three (the others are MD2 and MD4) have comparative structures, yet MD2 was upgraded for 8-bit machines, in examination with the two later recipes, which are advanced for 32-bit machines. The MD5 algorithm is an expansion of MD4, which the basic audit observed to be quick, yet conceivably not completely secure. In correlation, MD5 is not exactly as quick as the MD4 algorithm, but rather offers a great deal more confirmation of information security.

MD5 algorithm consists of 5 steps:

Step1. Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits fewer than a multiple of 512.

Step2. Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rules of appending length are:

- The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low-order word is appended first and followed by the high-order word.

Step3. Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value. The rules of initializing buffer are:

- The buffer is divided into 4 words (32 bits each), named as A, B, C, and D.
- Word A is initialized to: 0x67452301.
- Word B is initialized to: 0xEFCDAB89.
- Word C is initialized to: 0x98BADCFE.
- Word D is initialized to: 0x10325476.

Step4. Processing Message in 512-bit Blocks. This is the main step of MD 5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round.

III. LITERATURE SURVEY

Shivangi Goyal (2012) et al presented a precise study of cryptography, where it is applied and its utilization in diverse sorts [5]. Cryptography is a measure of protecting the essential data from unauthorized access. It has evolved as a safe way for transmitting information. It chiefly aid in restricting intrusion from third party. It provides data confidentiality, integrity, electronic signatures, and advanced user authentication. The approaches of cryptography employ mathematics for protecting the data (encryption and decryption). Author also examines a variety of cryptographic techniques and their particular region of applicability has been searched out and presented in summarized table form.

PranabGarg (2012) et al.[6] studied an current algorithm for securing data by encryption. Cryptography has been emerged as essential tool for data transmission. Various algorithms of cryptography has been studied, If advantages of all these algorithms are combined in one algorithm then performance of cryptography can be increased along with the length of key. In public key algorithm for generation of private key CDMA approach of communication can be used. Each user is provided a Different unique number called PN number and no other user is having that number. For each user this unique number is generated randomly and at the receiver end same PN number can be used to decrypt the message.

Mitali (2014) et al [7] provides a fair performance evaluation among the variety of cryptography algorithms on diverse settings of data packets. Author observed the encryption and decryption time of numerous algorithms on dissimilar sets of data. These encryption techniques support the performance of the encryption scheme also to guarantee the security proceedings. Here the performance evaluation of selected symmetric algorithms namely AES, 3DES, Blowfish and DES. Blowfish has better performance than other algorithms followed by AES.

AmbikaOad (2014) et al [8] present that In today's environment, security becomes an important issue in communication. For secure transmission of data in open network, encryption is very important methodology. Though encryption prevent our data from unauthorized access during transmission. Author surveyed various previous works which is used diverse approaches for image encryption and also provided general introduction about cryptography. In this paper, various important encryption techniques have been presented and analyzed in respect to compose common with the other encryption algorithms used in encrypting the image which has been transferred over network. The results of the simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images.

R.Nivedhitha (2012) et al [9] introduced two new approaches where in cryptography and steganography are combined to encrypt the data as well as to hide the data in different form by means of image processing. Hence securing the image by encryption, applying DES algorithm employing the key image. The encrypted image is hidden in different image by utilizing LSB scheme. The decryption can be done by the same key image employing DES algorithm. Here for encrypting secret image Data encryption standard is used and for hiding the encrypted image uses LSB technique into cover image. When steganography is combined with encryption a good security was obtained among two parties in case of secret communication, it is barely attracted from eavesdropper by naked eye. Lastly concluded that the devised scheme is efficient for secret data transmission.

Ms. Hemlata Sharma (2013) et al [10] here for encrypting a secret image employing BLOWFISH algorithm and comparing with other Algorithms. Now this encrypted image is embedded with video by using LSB Approach of steganography. Our proposed model gives two layers of security for secret data, which fully satisfy the basic key factors of information security system that includes: Confidentiality, Authenticity, Integrity and Non – Repudiation. Author worked on two major techniques of data security i.e. Cryptography and Steganography. These two techniques provide higher security to our data. Initially the information is encrypted by using Blowfish algorithm which is better than other encryption algorithms then the encrypted information is hidden by LSB approach. So it is very difficult for the unauthorized users to identify the changes in the stego image. The use of the blowfish algorithm and LSB gives a way to secure the information from illegal user and provide better PSNR value. In our paper we used a LSB to hide hidden image into video, which provides the new dimensions to the image steganography. It is very difficult to recover the hidden image for the third party without knowing the bits of the frames.

IV. PROPOSED WORK

1) For secure transaction we are using 3 DES with MD5 hashing algorithm in fingerprint image. For authentication we use OTP. In OTP we ask a question.

3DES or TDES:-

Is based on the DES (Data Encryption Standard) algorithm, therefore it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. As such, the DES algorithm itself has become obsolete and is no longer used.

MD5:-

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with digital signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. According to the standard, it is "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later formulas, which are optimized for 32-bit machines. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but offers much more assurance of data security.

Proposed algorithm:-

Encryption Process

1. MD5 algorithm computes 128 Bit MD5.
2. Reduce 128-bit message digest to 112 bits by discarding every number that is a multiple of 8-bit used for parity. This output is called as MD'.
3. Triple DES algorithm encrypts the Original Message (M) with help of MD' as symmetric key used in triple DES, and then produce a cipher text (CT).
4. The MD' Encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key(CK).
5. Combine a Cipher Text (CT) and Cipher text of Key (CK), produces a Complex Message (CM).Complex Message (CM) is sent to the Receiver B.

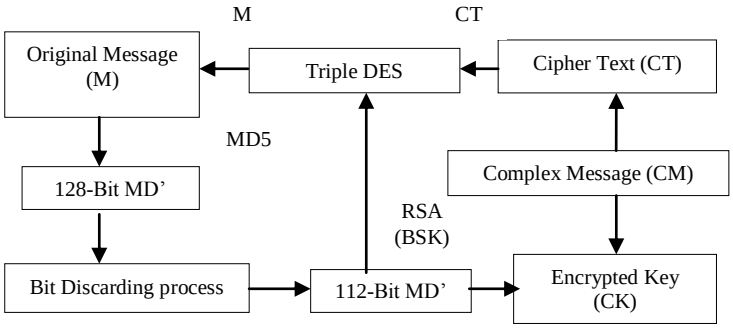

Figure. Encryption Process

A) Sender side encryption algorithm

1. Take text message M as input
2. Compute MD
   MD5(M)=MD
3. BDP(MD)=MD'
4. MD'=K
5. $E_K(M)=CT$
   $CT=E_{K1}(D_{K2}(E_{K1}(M)))$
6. Go to step 4
7. Encrypt key k with 3DES
   $E_{BPK}(k)=CK$
8. CK+CT=CM
9. Send CM to reciver

Decryption Process

1. The receiver B received cipher text CT into two parts, one is cipher text of key CK from the RSA algorithm encryption, and the other is cipher text CT from the triple DES algorithm encryption.
2. The receiver B decrypts cipher text of key CK by their own private key BSK, and retrieve the key K, then decrypt the cipher text CT to the original M by key K that is MD'.

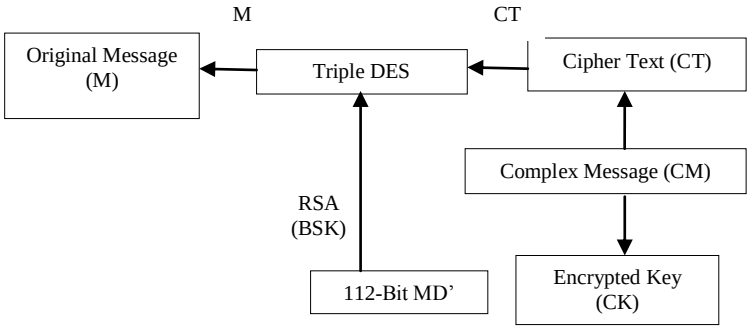

Figure. Decryption Process

B) Reciver side decryption algorithm

1. Recive CM
2. $D_{BSK}(CK)=K=MD'$
3. $D_K(CT)=M$
   $D_{K1}(E_{K2}(D_{K1}(CT)))=M$

V. SIMULATION AND RESULTS

Fig.3. Login details

In this figure user write email id and their password and then click on submit button for next process

Fig.4. Security system

In this figure start the security system.

Fig. 5 Registration Details

In this figure user register here and write user name,phone no, email id and plam image then click on submit button.

Fig. 6 Submission of user details

Here user submit their information

Fig.7 Generation of OTP number

Here system generates the OTP number for security session.

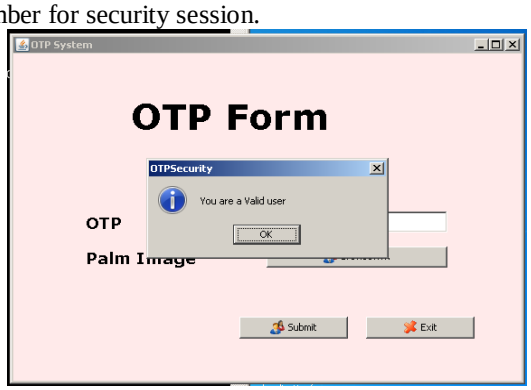

Fig. 8 Processing of OTP

Here show the valid user because of e mail and password.

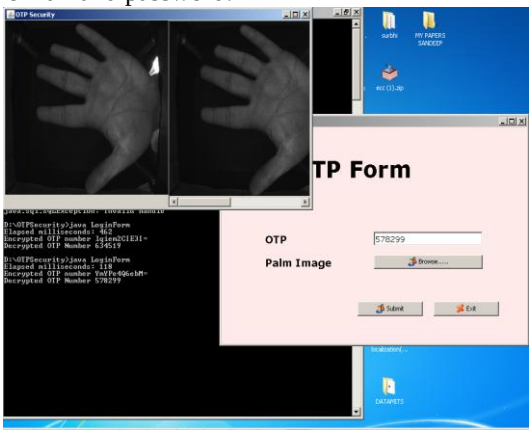

Fig. 9 Submission of OTP details of user

Here a form create and write OTP number which is already generated by system and palm image also then submit.

VI. CONCLUSION

Cryptography is an effective mean in securing e-commerce. . Cryptography is utilized to guarantee that the contents of a message are secrecy transmitted and would not be modified.

REFERENCES

[1] William stallings, ―Cryptography and Network Security:Principles& Practices‖, second edition,

[2] Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

[3] Mitali, Vijay Kumar and Arvind Sharma," Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 3, Issue 4, July-August 2014

[4] http://www.herongyang.com/Cryptography/MD5-Message-Digest-Algorithm-Overview.html

[5] ShivangiGoyal,"A Survey on the Applications of Cryptography", International Journal of Science and Technology Volume 1 No. 3, March, 2012 IJST,pp: 137-140.

[6] PranabGarg and Jaswinder Singh Dilawari," A Review Paper on Cryptography and Significance of Key Length", International Journal of Computer Science and Communication EngineeringIJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012,pp:88-91

[7] Mitali, Vijay Kumar and Arvind Sharma," A Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.orgVolume 3, Issue 4, July-August 2014, pp:307-3012

[8] AmbikaOad, HimanshuYadav, Anurag Jain," A Review: Image Encryption Techniques and its Terminologies", International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014, pp:373-376

[9] R.Nivedhitha and Dr.T.Meyyappan," Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012,pp:366-371

[10] Ms. HemlataSharma,Ms. MithleshArya, Mr. Dinesh Goyal,"Secure Image Hiding Algorithm using Cryptography and Steganography",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06 www.iosrjournals.org.

