TEST Engineering & Management

July-August 2020
ISSN: 0193-4120 Page No. 4443 - 4450

A Hybrid Cryptography Procedure to Achieve Security in Communication Network

***Nilima Karankar, **Vivek Kapoor**

Article Info
Volume 83
Page Number: 574 - 585
Publication Issue:
July-August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *10 August 2020*

Abstract

The digital communication technology offers efficient communication with low cost. It turn into much prevalent communication technique now a days. The internet based communication is one of the source of digital communication .The significant amount of data carries in network as well as some of the data is much sensitive and private. The attackers are tries to break the existing network security and recuperate the sensitive information. So there is necessity to enrich security during the network based communication. In our proposed work, using cryptographic technique the security is enhanced either by enhancing the technique of key generation or modification on the key policies or by improving the cipher generation process. In our work both kinds of improvements are made to improve the security of data using cryptographic techniques. The proposed hybrid cryptographic technique involves goodness of MD5 hash generation algorithm and the DES algorithm. The RSA algorithm is worn to encrypt the key and to defend it while data is traversed through communication network.. Then the cipher text and encrypted key is sent securely to the user in Digital Envelope. According to survey of different cryptographic techniques both the cryptographic techniques are proficient and sheltered for cipher generation purpose.

Keywords: *Cipher Text, Data Encryption Standard (DES), Message Digest (MD), RSA;*

I. INTRODUCTION

Security is an important apprehension in digital data communication. A sum of different sort of attack are installed in the public networks due to which loss of money, reputation and data is observed. Hence, a safe and sound process of communiqué is required. In this paper our work is likely to find the clarification for enhanced security of communication in the digital world.

The internet is industrially highly developed and more prevalent in recent years; numbers of new users are increasing day by day in this platform. Almost all the users directly or indirectly use the services of internet either for financial transactions, messaging or for information gathering etc. Due to this a noteworthy amount of private or confidential data is traveling through the internet network. On the other side different kinds of network attacks are also spotted and increasing day by day. Thus there is prerequisite to prevent the attackers to obtain the access to the important confidential data by using some security techniques.

There are number of different security techniques available to provide security to the network communication. A large number of them are either feeble secure or are not effectively efficient. In the field of secure communication, cryptography (encryption/decryption) plays an important role. The cryptography prevents the various attacks to break confidentiality, authenticity, integrity of the sender. Therefore almost all the features of security the cryptographic (encryption/decryption) techniques are used. The cryptographic techniques known are straightforward to put into operation and are cost effective. It is seen that traditional cryptographic techniques are losing their reliability, as their procedures are common and the attackers know very well about them. Thus in our work a secure hybrid cryptographic procedure is introduced for securing the network communication in public domain.

II. RELATED WORK

This section covers about the recent and commendable work done by various researchers and academicians to enhancing the domain of secure communication in an unsecured network. Thus the work done in different research papers and articles are account in this section.

Nilima Karankar,et al In propose a combination of MD5 with asymmetric and symmetric key cryptography to provide all security features. In order to provide all security feature at one place a unique digital envelope is proposed, which comprises of digital signature and best of both the world and providing security features like integrity and all by using Blowfish and RSA (Ron Rivest Shamir Adelman) algorithm in join up with MD5. Which result in , overcome the deficiency of current digital envelope technique and strengthens the security of public network.

Parsi Kalpana et al applied cryptography in cloud computing domain. Even if the Cloud Computing is competent and regimented, there are many glitches for the data security as there are no proper procedures for the Cloud user. To make certain the security of data, author projected a technique by implementing RSA algorithm.

Seema Rani et al introduced an superior version of AES Algorithm which is an mixture of AES and neural networks. The overall work provides us the enhanced recital over AES in edict to augment security.

In modern era network security has become a very important concern. Many procedures are urbanized to safeguard the collective data. **Prerna Mahajan et al** spotlight on cryptography to defend the data while get across in the public network. In this paper author has put into practice three encryption technique like AES, DES and RSA algorithms and evaluator against recital based on the assessment of its time at the moment of encryption and decryption. Efficiency of each algorithm is scrutinized. Amalgam i.e hybrid or mixture of encryption algorithm in combination with symmetric key and asymmetric key cryptography is the real solution. **Komal Rege et al** projected hybrid encryption algorithm, AES algorithm is used to encrypt plain text, and RSA algorithm for the encryption of the AES key. Thus the dual security will make the data transmission more safe using Bluetooth and less overheads.

Kapoor V et al offers a safe and sound cryptographic practice which guarantees a extremely secure cipher creation modus operandi using the RSA, DES and SHA1. The implementation of the projected system was done using the JAVA technology and their recital in terms of space and time intricacy is evaluated with the traditional RSA cryptography. The projected cryptographic technique was found the competent and improved cipher text was obtained during relative presentation psychoanalysis.

Kapoor Vivek et al proposes which encrypt and decrypt message with clandestinely generated sender key and receiver key which is shared by sender and receiver. Two level of security is put into practice.

Anshu Parashar et al have discuss about cloud computing safety challenges, methods, measures, that cloud service provider visage during cloud engineering and currented the allegorical study of varied security algorithms.

A survey of various Encryption Algorithms is presented by **Gurpreet Singh et al** In recent years, with the farfetched maturity of knowledge exchange in network environments and increasing the attacker’s capabilities, information security has became the foremost significant procedure for data storage and communication. In edict to supply such information security the confidentiality, data integrity, and data origin authentication must be qualified supported cryptography. **Disha Shah** explains cryptographic algorithm named as Message Digest Algorithm. It generates digital signature using MD5 algorithm to defend the information.

Ruchi Rajkumar Bajpai et al propose a secure data retrieval scheme using Triple DES with MD5 for decentralized encryption where multiple key authorities manage their attributes independently. **Ivan Del Pozo et al** proposes a replacement symmetric encryption mechanism for instant text messaging in mobile devices. Their mechanism uses a sequence of prime numbers obtained from a bi-dimensional matrix and a secret key for the encryption process. The suggested solution has been compared with other well-known symmetric and asymmetric algorithms. Results show that symmetrical mechanisms are more efficient for fast messaging.**Zhong-Hua Pang et al** addresses the safety problems with data transmitted in networked control systems (NCSs), especially confidentiality, integrity and authenticity. A secure networked predictive system SNPCS architecture is obtainable , which integrates the confidentiality, integrity, timestamp strategy, and recursive networked predictive control (RNPC) method.

OBJECTIVES

The main aim of the work done is to find the competent and locked cryptographic technique to shelter the network based communication in the public domain. Therefore a digital based application for communication and cryptographic approach demonstration is used. The proposed technique accomplishes the objectives which were discovered during the study. Study of different cryptographic approaches is done. In addition to its new techniques for enhancing the cryptographic security is also studied. Design and execution of hybrid cryptographic technique and planned approach is make available. To design the required technique the system architecture and algorithm process is presented. A hybrid encryption algorithm in which comprises of symmetric, asymmetric and hash algorithms applied in various permutation and combinations to achieve various security features. Performance of the proposed cryptographic technique is evaluated for finding the methods efficiency. Thus the different performance parameters such as time and space complexity of the proposed algorithm are to be computed and reported.

This section provides the understanding about the core objectives and the aim of study, in further section the background and problem domain is discussed. .

III. PROBLEM DOMAIN

In this age of information technology a lot of data is transmitting with the help of networks. Sometime data is traveled in unknown not so secure environment i.e public networks and these networks are not much trusted for secure data exchange. Therefore the following issues are considered for further investigation and system development.

1. Communication in un trusted environment
2. Improve the security and complexity of data security
3. Improve the performance of the digital envelops.
4. Extend the work for more than one format such as audio and video
5. The proposed working model for the cryptographic data security for the not trusted network is demonstrated using figure 1.1. In this diagram the encryption process of the algorithm and decryption part of the proposed algorithm is explained. Therefore the proposed technique is designed in two major modules first (Upper part) is encryption and second (Lower part) is the decryption. Both the aspects of the proposed system are described as under:

A. ENCRYPTION PROCESS

In the proposed cryptographic function the three major phases are implemented in iterative manner. In initial step the input data which is denoted as I/P data for the further documentation is produced to the cryptographic system. As the data I/P data is found in system the MD5 hash generation algorithm is applied to data I/P data and 128 bit key is prepared that is termed here as . The Key and the data D I/P data is produced to the DES algorithm that processes the data in first phase and generates the cipher text. In second phase it is again produced to the MD5 algorithm for generating the key. This key and cipher text of first phase is produced into the DES algorithm for generating the new cipher text. Similarly in third phase the key and cipher text is generated.

Now for transmission the keys are appended and processed using the RSA algorithm. Here for RSA 1024 bit key is used to generate a new cipher text. Finally the DES based cipher text are combined and send for transmission.

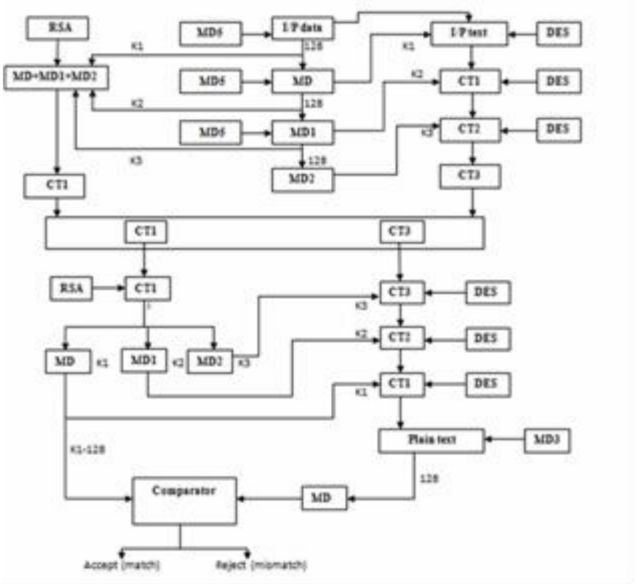


Figure 1.1 Proposed System

B. DECRYPTION PROCESS

On the other hand the combined cipher text of the proposed cryptographic technique is arrived on the receiver end. The receiver first decrypts the cipher using the RSA algorithm and generates the cryptographic keys namely. Now this provided to DES algorithm with the key to generate the cipher. In next and is produced to the DES for finding the. And finally the key is used to find the original text. After recovering the original text the data is again processed using the MD5 algorithm and that generates the a 128 bit hash code here that is denoted as K. this generated hash K and the initial key is compared. If both the hash codes are similar then the data is accepted by the receiver otherwise the data rejected.

V. RESULT ANALYSIS

Therefore the time and space intricacy of the proposed algorithm is computed and demonstrated in this section.

A. TIME COMPLEXITY

The algorithm consumes a fraction of your time for computing the encryption or decryption process. that point is termed here because the time consumption of the system or time complexity of the algorithm. The time consumption of the algorithm is computed using the subsequent formula.

Data files	Encryption	Decryption
10	12.4	10.37
30	17.37	15.26
50	24.28	20.74
100	37.51	32.19
200	42.33	40.95
500	67.71	61.04
800	81.47	76.21

Table 5.1 time consumption

Figure 5.1 time consumption

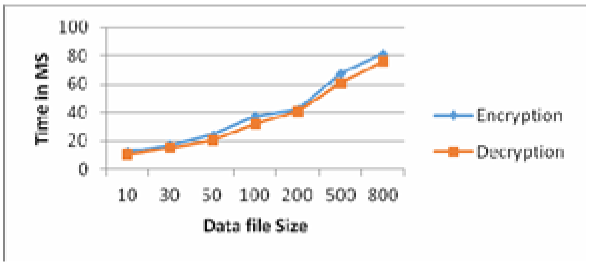
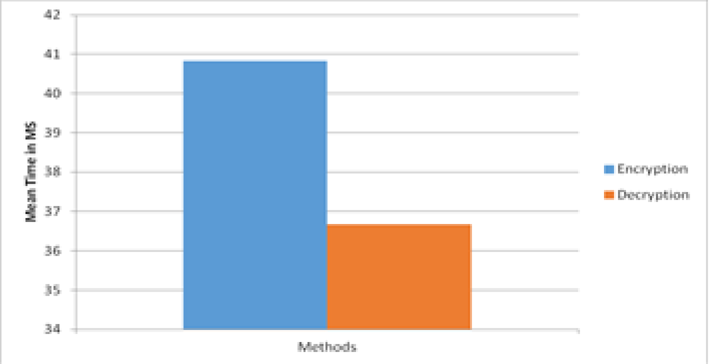


Figure 5.2 mean time complexities



The figure 5.1 and table 5.1 shows the time intricacy of the algorithm is demonstrated in terms of encryption and decryption. In this diagram for encryption process the blue line is used and the red line is used to show the performance of decryption algorithm The diagram contains the file size for experimentation in X axis and therefore the Y axis shows the time of execution in terms of milliseconds. According to the obtained results of the algorithm the encryption and decryption algorithms consumes similar amount of time but the time consumption for the encryption process is slightly higher than the decryption time. Additionally the time utilization of the algorithm is increases as the amount of file size for experiments are increases. According to the obtained performance results the decryption algorithm is 4 MS faster than the encryption algorithm.

B. SPACE COMPLEXITY

The amount of main memory size required to execute an algorithm is termed as the space complexity or the memory utilization of algorithm. The memory utilization of any algorithm can be measured by the following formula.

Data files	Encryption	Decryption
10	26847	26199
30	27163	26918
50	27829	27719
100	28947	29183
200	29410	29371
500	30194	29914
800	30913	29186

Table 5.2 space complexity

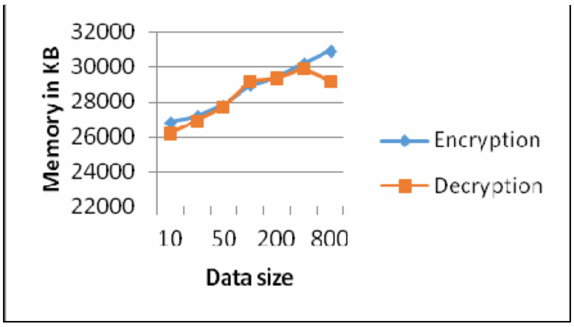


Figure 5.3 space complexity

The figure 5.3 and table 5.2 shows the main memory requirements of the proposed algorithm for encryption and decryption. The X axis of the diagram contains the amount of file size in terms of KB and the Y axis show the amount of main memory required in terms of KB. To demonstrate the performance of the implemented algorithm blue line is used for encryption memory requirements and the red line shows the decryption memory requirements. According to the obtained results the encryption algorithm needs higher memory as compared to the decryption memory utilization. In addition of that the memory requirements of the algorithm is increases with the size of input file for encryption and decryption.

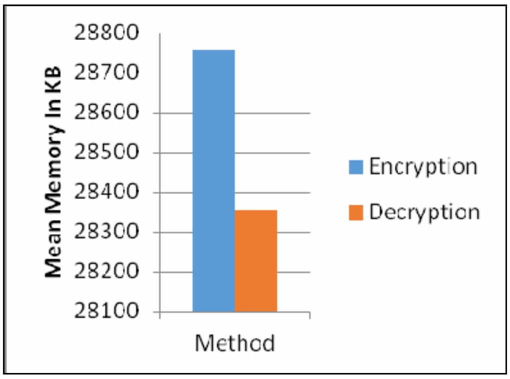


Figure 5.4 mean memory consumption

The mean performance of the algorithm in terms of memory requirements are also computed and reported using the figure 5.4. In this diagram the X axis shows the encryption and decryption methods and the Y axis contains the mean memory consumption of the system. According to the obtained performance the decryption algorithm also consumes less memory as compared to the encryption algorithm. The memory consumption in decryption is approximately 400KB lower than encryption algorithm.

VI. CONCLUSION

The digital data communication and their requirements are increasing in a rapid manner. In addition of that every day new users are also interacted with this channel of communication. In different communication technology the internet is one of the most important and popular technology. There are a number of applications that are served through this technology such as online banking, ecommerce web stores and others. These applications need the sensitive and private data for accessing their accounts online. But the internet network is a kind of public network and not much secure intermediately due to man in middle attacks and others. For providing protection to the data in communication network some cryptographic techniques are used.

In this presented work the cryptographic data security techniques are studied and a new technique using the hybrid concept of cryptography is proposed. The cryptography is a process in which the security is enhanced in two different manners, either by modifying the approach using different similar technique or improves the key generation process. In this presented technique both the aspects of the security is considered. The proposed technique involves the three different algorithms in three passes. The algorithms are MD5, DES and RSA algorithm. Among the DES and MD5 algorithm is used to encrypt and decrypt and provide integrity to the input data produced by the user. And the RSA algorithm is implemented for securing the keys of encrypted data for data recovery. The proposed concept encrypts the data three times with the different keys therefore the generated cipher is much complex and secure during the public network transmission.

JAVA Technology is used to implement the proposed security technique. Additionally for finding their effectiveness the performance of the cryptographic technique is evaluated with respect to time and space complexity. The obtained performance of the proposed cryptographic technique for internet based file transmission system is summarized using the table 6.1.

S. No.	Parameters	Encryption	Decryption
1	Time Complexity	High	Low
2	Space Complexity	High	Low

Table 6.1 performance summary

According to the obtained performance the proposed technique is efficient and consumes fewer resources for cryptographic process. Thus the method is adoptable for securing the file transmission and storage techniques over the network based applications.

VI. REFERENCES

1. Nilima Karankar, V. Kapoor, “Locked Digital Envelope System Grounded on Hash Function for Providing Key Security Features” Published in CiiT International Journal of Automation and Autonomous System Volume 7 Issue 02, pp 44-50. March 2015 ISSN 0974 – 9659.
2. Parsi Kalpana, Sudha Singaraju, “Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
3. Seema Rani, Dr Harish Mittal, “A Compound Algorithm Using Neural and AES for Encryption and Compare it with RSA and existing AES”, Journal of Network Communications and Emerging Technologies

(JNCET) www.jncet.org Volume 3, Issue 1, July (2015).

4. Dr. Prerna Mahajan & Abhishek Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.
5. Komal Rege, Nikita Goenka, Pooja Bhutada, Sunil Mane, “Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA”, International Journal of Computer Applications (0975 – 8887) Volume 71– No.22, June 2013.
6. Vivek kapoor Rahul Yadav. “A Hybrid Cryptography Technique to Support Cyber Security Infrastructure” Published in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 11, November 2015. pp 3995-4002 ISSN: 2278 – 1323.
7. V. Kapoor, Rahul Yadav “A Hybrid Cryptography Technique for Improving Network Security” Published in International Journal of Computer Applications Vol. 141, No. 11 , May 2016. pp 25-30 ISSN: 0975-8887. UGC Approved journal No. 44570. https://www.ijcaonline.org/archives/volume141/number11/kapoor-2016-ijca- 909863.pdf
8. Anshu Parashar, Rachna Arora, “Secure User Data in Cloud Computing Using Encryption Algorithms”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.
9. Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013
10. Disha Shah, “Digital Security Using Cryptographic Message Digest Algorithm”, International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 10, October 2015
11. Ruchi Rajkumar Bajpai, Prof. P.S. Kulkarni, “COLLOBORATIVE APPROACH for SECURING DATA RETRIEVAL SCHEME BASED On TRIPPLE DES with MD5 for DECENTRALIZED DISRUPTION TOLERANT MILITARY NETWORK”, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763 Issue 06, Volume 3 (June 2016)
12. Ivan Del Pozo and Mauricio Iturraldea, “CI: A New Encryption Mechanism for Instant Messaging in Mobile Devices”, International Workshop on Mobile Computing Security (MCS 2015), 2014 The Authors. Published by Elsevier B V
13. Zhong-Hua Pang and Guo-Ping Liu, “Design and Implementation of Secure Networked Predictive Control Systems Under Deception Attacks”, IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, VOL. 20, NO. 5, SEPTEMBER 2012.

AUTHORS PROFILE

Author-1
Photo

Nilima Karankar pursed Bachelor of Engineering from Mandsaur Institute of Engineering, Mandsaur in year 2006 and Master of Engineering from Institute of Engineering and Technology, DAVV INDORE in 2015. And currently working as Assistant Professor in Department of Computer Engineering, Institute of Engineering and Technology, DAVV INDORE since 2006. I was a member of ACM since 2011-2015. I had published 7-9 research papers in reputed international journals and it’s also available online. My main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy,Artificial Intelligence based education. I have 12 years of teaching experience..

Author-2

Dr Vivek Kapoor is working as Assistant Professor in Information Technology Department at Institute of Engineering and Technology, Devi Ahilya University, Indore, India. He Received Bachelor of Engineering (B.E.) from Pt. Ravishankar Shukla University, Raipur, Chattisgarh and Master of Technology (M. Tech) & Ph. D Degree in Computer Science degree from Devi Ahilya University, Indore. He has over 13 years of experience in teaching various courses like B.E., M.E., MBA and MCA. He has been teaching various subjects like Data Structures, Database Management System, Computer Networks, Information Security and Programming Languages. His research interests include Computational Finance, Genetic Algorithms and Data Mining. He has got three research papers to his credit in International journals and three in Internationnal conferences on the above topic.