International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 716-720 Jan 2019-June 2019 www.csjournals.com

RSA and XOR Base Encryption Mechanism to Secure the Cloud

[1]Sandeep Singh, [2]Dr Vishal Verma
[1]Research Scholar, [2]Asst. Professor
Deptt. Of computer science and application, Chaudhary Ranbir Singh University, Jind, Haryana, India

Abstract: Here, encryption and decryption of information has made using RSA and XOR. The proposed technique is more secure and more efficient as compare to traditional security technique. The use of XOR operator has enhanced the security of network. XOR key would encrypt data more efficiently as compare to traditional algorithm. The Proposed technique makes the data transmission fast. The proposed technique is more secure in all sense as it is immune to brute force attack as well as timing attack. The XOR based security has been improved the performance of encryption and decryption. Additional security technique such as IP verification restricts the attacks from hacker end. In this research real image is loaded for encryption. The key image is then loaded to perform XOR operation From above results in case of timing attack comparison of traditional and proposed work, it is clear that the strength of proposed work as compare to traditional RSA work. From the above analysis it has been clear that the probability of Timing attack is more in case of tradition RSA.

Keywords: RSA, XOR Encryption, Decryption, IP Filter.

[1] Introduction

RSA has been determined *as* one of the first public-key cryptosystems. It has been used to secure the dealing of information the key to encrypt the data is public in such a cryptosystem. This key is separate from the key which is used to do the decryption of data. This key is kept secret. With RSA, this asymmetry is dependent on actual complexity of factorization. This is related to the product of two large prime numbers. RSA user formulates a public key after that he publishes this key. This key is made on the base of two large prime numbers. This key also considers an auxiliary value. It is vital that the user kept this prime numbers private. Everyone who knows about the public key is used to do the encryption of a message. Therefore some techniques are published presently. If there is a proper length of public key, in that situation the knowledge full person of prime numbers can made decoding of the data. In the situation in which anyone breaks the RSA encryption is referred as RSA problem.

[2] Encryption and Decryption Algorithm of RSA

Two keys, d and e are used in RSA algorithm. It has been used to for decryption and encryption, respectively. The actual data P has been encrypted into decoded form that is referred as cipher text C.

Algorithm of RSA for encryption

Following step are include in order to RSA encryption in text

STEP1:-Take plane text P
STEP2:- Take two keys d and e
STEP3:-Take n constant
STEP4:- Get cipher text using equation $C = P^e \bmod n$

Algorithm of RSA for decryption

Following step are include in order to RSA decryption in text

STEP1:- Take Cipher text C
STEP2:- Take two keys d and e
STEP3:- Take n constant
STEP4:- Get plain text using following equation $P = C^d \bmod n$

[3] OBJECTIVE

The following are the objectives of the under reference research work:

1. Study and analysis of existing steganography security technique.
2. Identification of loopholes in existing security technique.
3. Design of proposed steganography technique to enhance the security with IP filter security technique and using the concept of visual steganography.
4. Designing secure encoding and decoding technique to enhance the protection of system using the concept of visual steganography.
5. Performance comparison between proposed XOR techniques with the existing One.
6. Study of Brute force attack and Timing Attack and conclude how the proposed technique would enhance security from brute force attack

[4] RESULT AND DISCUSSION

RSA BASED IMPLEMENTATION IN MATLAB

Fig 1:- crypt.m (part 1)

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 716-720 Jan 2019-June 2019 www.csjournals.com

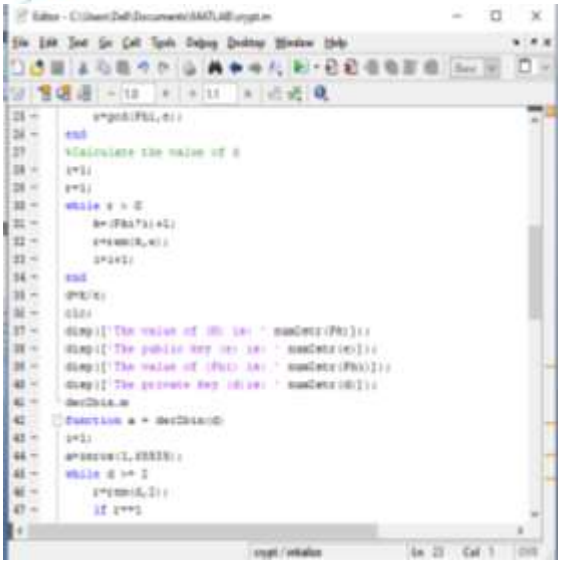

Fig 2 crypt.m (part 2)

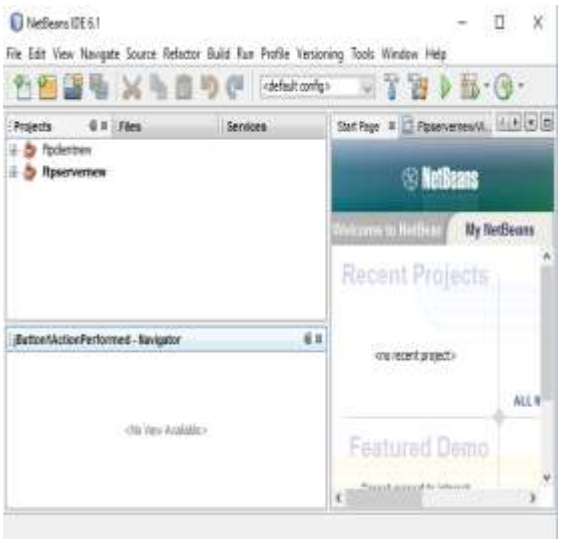

Fig: 3 Server Side designing and written code to enable download option and disable download option

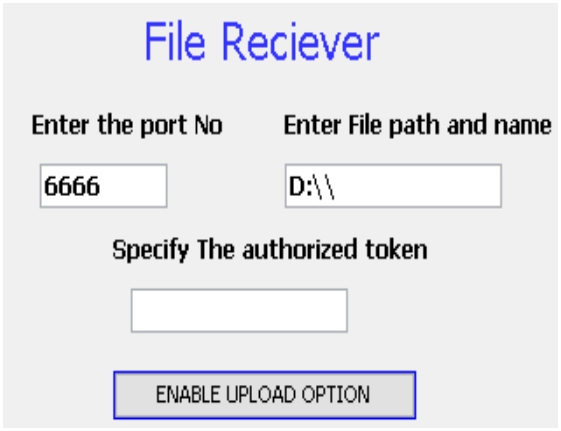

Fig: 4 Design view of Receiver application

Table 1 Difference between Time Taken In Case of Traditional Security System and Proposed System

No of Packets	Time taken in case of Existing/traditional	Time taken in case of proposed work
10	1	0.7
20	1.8	1.4
30	2.4	1.9
40	3.2	2.6
50	4	3.1
60	5	3.7

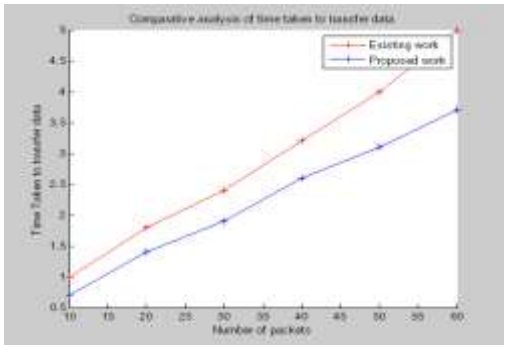

Fig 5 Comparative analysis of time taken during transmission

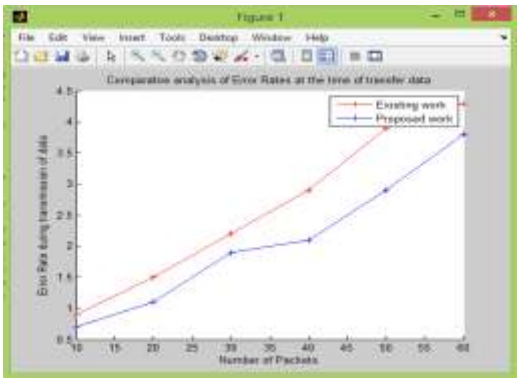

Fig 6 Comparative analysis of error rates at time of transfer data

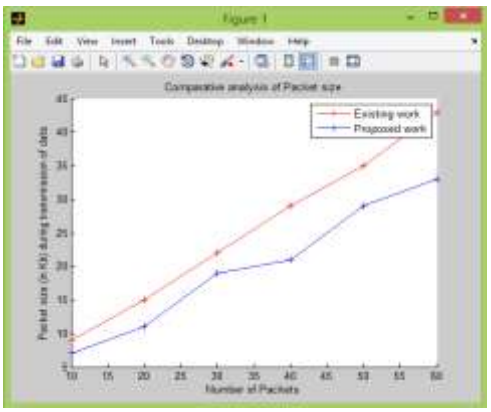

Fig 7 Comparative analysis of packet size

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 716-720 Jan 2019-June 2019 www.csjournals.com

Table 2 Comparison between traditional RSA and proposed XOR technique

Parameter	Tradition RSA Technique	Proposed XOR Technique
Brute force attack	Attack is possible	Attack is not possible
Timing attack	Possible of timing attack	No possibility of timing attack
Port	Predefined	User defined
Security	LESS secure because suffer from brute force and timing attack	MORE secure because no chance of brute force and timing attack
Ip validation	NO	YES
Multi level encryption	NO	YES

Table 3 Comparative Analysis In Case Of Brute Force Attack

No of packets	TRADITIONAL RSA Technique	PROPOSED TECHNIQUE
100	6	1
200	8	2
300	12	4
400	15	6
500	22	9
600	31	13
700	42	18
800	51	23
900	63	28
1000	72	32

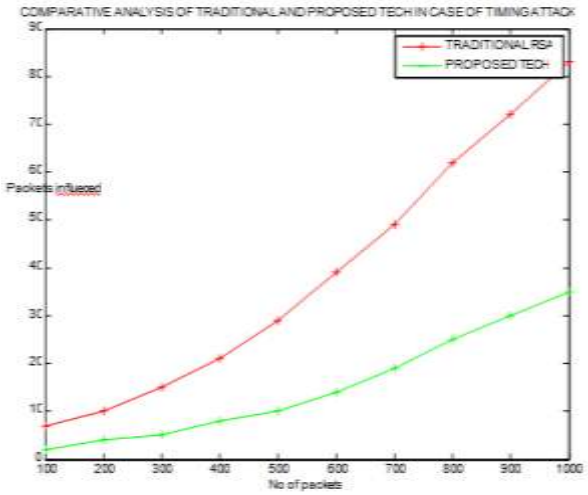

Fig 8 comparative analysis of traditional and proposed technique in case of Brute force attack

Table 4 Comparative Analysis of Traditional and Proposed Technique In Case Of Timing Attack

No of Packets	Traditional RSA Technique	Proposed XOR Technique
100	7	2
200	10	4
300	15	5
400	21	8
500	29	10
600	39	14
700	49	19
800	62	25
900	72	30
1000	83	35

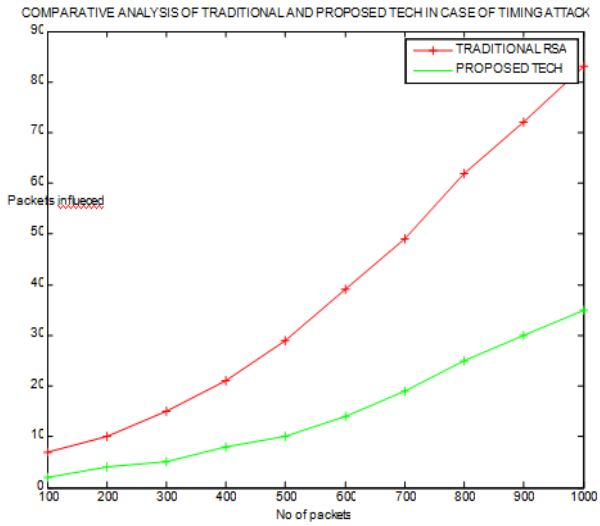

Fig 9 Comparative analysis of traditional RSA and proposed XOR technique in case of Timing Attack

[6] CONCLUSION

From above results in case of timing attack comparison of traditional and proposed work, it is clear that the strength of proposed work as compare to traditional RSA work. From the above analysis it has been clear that the probability of Timing attack is more in case of tradition RSA. As the number of packet increase, the probability of timing attack enlarges. Chances of unauthentic data access from Timing attack in proposed technique is less in proportion to traditional when then packet got increased. The proposed technique is more secure in all sense as it is immune to brute force attack as well as timing attack. The XOR based security has been improved the performance of encryption and decryption. Additional security technique such as IP verification restricts the attacks from hacker end. In this research real image is loaded for encryption. The key image is then loaded to perform XOR operation.

[7] FUTURE SCOPE

The research work would be beneficial to secure data from RSA attack as the probability of Brute force attack is more in case of tradition RSA. It would also be beneficial to save data from Timing attack as the probability of timing attack is more in case of previous RSA. As packet increases, the probability of timing attack also increases. Threat of attack on data using timing attack in proposed technique would be negligible as compare to traditional when then number of packet increases. The project scope is that it would limit the unauthorized execution. It would offer the better protection at the time of data transmission.

REFERENCE

[1]. Erin Michaud(2003) "Current Steganography Tools and Methods", SANS Institute 2003, As part of GIAC practical repository, GSEC Practical, Version 1.4b April, 2003

[2] A. Perrig, J. Stankovic, and D. Wagner,"Security In Wireless Sensor Networks,"ACM,Vol. 47, No.653.2004.

[3] H. Anderson. Introduction to Computer Security, Prentice Hall, 2004,pp: 85-86

[4] Kristin Lauter,"The Advantages of Elliptic Curve Cryptography for Wireless security", IEEE Wireless Communication, Feb 2004.

[5] Z.Z Kermani and M. Jamzad. "A robust steganography algorithm based on texture similarity using Gabor filter." in Proc. of IEEE 5th International Symposium on Signal Processing and Information Technology ISSPIT, 2005. pp. 578-582.

[6] A.I. Hashad, A.S. Madani and A.E.M.A. W ahdan. "A robust steganography technique using Discrete Cosine Transform insertion." In Proc. of IEEE/ITI 3rd International Conference on Information and Communications Technology, 2005. pp. 255-264.

[7] X. Zhang, and S. Wang,"Efficient steganographic embedding by exploiting modification direction, "Communications (Volume:10 , Issue: 11) November 2006,page(s):781-783.

[8] A. Savoldi, and P. Gubian,"Data hiding in SIM/USIM cards: A steganographic approach,"Systematic approaches to digital forensic engineering, 2007. SADFE 2007. second international workshop on 10-12 April 2007,page(s):86-100.

[9]Vivek Kapoor et al., "Elliptic Curve Cryptography," ACM Ubiquity, Volume 9,Issue 20,(20-26)-may-2008.

[10].F. Amin, A. H. Jahangir and H. Rasifard,"Analysis Of Publickey Cryptography For
Wireless Sensor Networks Security,"In Proceedings of World Academy of Science,
Engineering and Technology, ISSN 1 307-6884,2008

[11] Dipti Kapoor Sarmah1, Neha Bajpai (2009) "Proposed System for data hiding using Cryptography and Steganography",

[12] Dragoş Dumitrescu1, Ioan-Mihail Stan1, Emil Simion (2009) "Steganography mechanism",

[13] George Abboud (2010) "Steganography & Visual Cryptography in Computer Forensics " 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering

[14] Masoud Nosrati, Ronak Karimi (2011) "An introduction to Steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195

[15] Pranab Garg, Jaswinder Singh Dilawari (2012) "A Review Paper on Cryptography and Significance of Key Length", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012

[16] Pria Bharti, Roopali Soni (2012) "New Approach of information Hiding in graph with the use of Cryptography and Steganography ", IJCA. Volume 58– No.18, November 2012

[17] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay (2013) "Review and Analysis of Cryptography mechanism", International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013

[18] C.P.Sumathi, T.Santanam and G.Umamaheswari (2013) "A Study of Various Steganographic mechanism using for data Hiding", IJCSE Vol.4, No.6, Dec. 2013

[19] Rakhi1, Suresh Gawande (2013) "A Review on Steganography Methods", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013

[20]Anjula Gupta Navpreet Kaur Walia (2014) " Cryptography Algorithms: A Review", 2014 IJEDR | Volume 2, Issue 2 |

[21] Vikas Yadav Vaishali Ingale Ashwini Sapkal and Geeta Patil (2014) "Cryptographic Steganography ", Computer Science & Information Technology

[22] Mr. Falesh M. Shelke1, Miss. Ashwini A. Dongre (2014) "Comparison of different mechanism for Steganography in images", International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 2, February 2014

[23] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal(2014) "A Review on Different Image Steganography mechanism", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014

[24] Souvik Roy and P. Venkateswaran (2014) "Online Payment System with the use Steganography and Visual Cryptography", 2014 IEEE.

[25] Sana Shiva, A.Hari Teja (2015) Secure E-marketing Using Steganography & Emergence of Cryptography Journal of Computer Science & Information Technology IJCSMC, Vol. 4, Issue. 1, January 2015, pg.532 – 538

[26] S. R. Navale1 , S. S. Khandagale, R. A. Malpekar3, Prof. N. K. Chouhan4 (2015) Approach for Secure Online transaction using Visual Cryptography & Text

Steganography International Journal of Engineering Research & Technology (IJERT) Vol. 4 Issue 03, March-2015

[27] Pradnya S. Nagdive (2015) Visual Cryptography & Steganography : A Review International Journal of Advance Research in Computer Science & Management Studies Volume 3, Issue 1, January 2015

[28] S.M.Poonkuzhali1 , M.Therasa (2015) "Data Hiding Using Visual Cryptography for Secure Transmission", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2015

[29] Archana.O.Vyas, Sanjay.V. Dudul (2015) "An Overview of Image Steganographic mechanism", International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015

[30] Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar,A. M. Bagul (2016) Online Payment System using Steganography & Visual Cryptography, International Journal of Computer Engineering In Research Trends, Volume 3, Issue 4, April-2016, pp. 157-161

[31] K.S.Seethalakshmi (2016) "Use of Visual Cryptography and Neural Networks to Enhance Security in Image Steganography ", IOSR Journal of Computer Engineering Special Issue - AETM'16

[32] A. Joseph Amalraj1, Dr. J. John Raybin Jose (2016) "A Survey Paper on Cryptography mechanism", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016, pg. 55-59

[33] Priyanka Bubna, Anshula Panchabudhe, Pallavi Choudhari (2017) "Review on Implementation Visual Cryptography & Steganography for Secure Authentication", International Research Journal of Engineering and Technology Volume: 04 Issue: 02 | Feb -2017

[34] Priyanka B. Kutade, Parul S. Arora Bhalotra (2015) "A Survey on Various Approaches of Image Steganography ", International Journal of Computer Applications Volume 109 – No. 3, January 2015

[35] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceeding of IEEE Students' Conference on Electrical, Electronics and Computer Science , Jadavpur University, Kolkata-700032, India, 2014.

[36] Thiyagarajan, P. Venkatesan, V.P. Aghila, G. "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE, 2010.

[37] N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, ,Client-side defense against web-based identity theft,' in Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp, San Diego, CA, Feb. 2005.

[38] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3,n 4, October/December 2006.

[39] Odai M. Al-Shatanawi and Nameer N. El. Emam (2015) "A new image Steganography algorithm dependent On mlsb method with random pixels Selection", IJNSA, Vol.7, No.2, March 2015.