EFFECTIVE USE OF BLOWFISH ALGORITHM IN ANALYZING SYMMETRICAL KEY CRYPTOGRAPHIC ENCRYPTION

V. Joseph Emmanuvel, E. J. Thomson Fredrik*

Abstract

Normally, the algorithms available in cryptography necessitate the keys that have to be shared and keep up relationship among the keys. The ultimate aim of allocation of keys is to atain an approved algorithm with very excellent arrangement of keys. RSA procedure is normal but a good number imperative hazard using the same is augmentative and for this reason does not promise distinctiveness of the key by not standing factual to the system requirements. In the event of getting better restrictions in the hand structure, a new cryptographic scheme of organizing the keys has to be proposed that brings into play the symmetric key procedure (Blowfish). Additionally, the suggested work makes use of ant colony based developmental computing technique to convene the necessity where there are changes in the key vigorously maturing with the time and the proposed method is found to be speedy and secured. A chronicle encompassing this method on a communication network has been implemented and another example of power saving is observed and the system is competent enough to meet the security necessities of modern networks.

Keywords : Symmetric Cryptography, Shared Key, Blowfish, Encryption, Decryption, RSA

I. INTRODUCTION

To make the availability of security and defending information has turned out to be a very complicated mission. Every organization should contain diverse strategies concerning to data safety. To afford security, convinced algorithms and tools have to be put into practice. In the event of ever-increasing insist for information security, image encryption and decryption has developed into an imperative research neighborhood and it has extensive application scenario. Image security is a supreme concern because web attacks happen to be severe.

In [1], Mr. Rajesh Et al completed a detailed evaluation on attacks and encryption tools and mentioned that cryptography plays a major responsibility in providing security when the message is transmitted. In [2], Mrs. Smita Desai, Et al discussed a Blowfish Algorithm where encrypting and decrypting image contains claims in internet communiqué and multimedia system. In [3], Anjaneyulu GSGN Et al made a survey using blowfish algorithm with random number generator. The nosy human beings attempt to rupture the non readable message but it is tough to accomplish it. In [4], Anjula Gupta, Et al published an article on algorithms on cryptography and proposed that recent cryptography is profoundly on the base of mathematical conjecture and computing science practice. Blowfish affords a superior encryption tempo in software and it has been the best effective cryptanalysis till date.

In [5], Ayushi, Et al explained a symmetric key cryptographic algorithm called blowfish which is a symmetric key block cipher including a bulky number of cipher matching sets and encryption products. To improve the performance of encryption and decryption, a secret key block cipher called 64- bit blowfish is an evolutionary improvement over Data Encryption Standard and triple DES. This algorithm is used as a changeable key size up to 448 bits. It makes use of the Feistel set-up which iterates undemanding function 16 times [6].

II. LITERATURE SURVEY

There are two most important types of encryption techniques in cryptography, they are Symmetric and asymmetric.

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore Tamilnadu, India
*Corresponding Author

Symmetric and Asymmetric Encryption

Symmetric encryption is a shape of cryptosystem in which encryption and decryption are executed using the identical key which is in additionally recognized as conventional encryption. These practice converts original text into cipher text using an undisclosed key and an encryption algorithm. Using the similar key and a decryption algorithm, the actual text is recovered from the cipher text [7]. The input for this encryption has been a statistics string that is nourished by the encrypted text for the purpose of moving the data speedily and makes it encrypted. The most beneficial of this method is, the input is entirely arbitrary, but there are techniques to obtain keys from passwords. Most risky branch of exercising this encryption is to stock up the key and make it accessible to the software that requests it. It is furthermore referred to as secret key [8]. Asymmetric encryption is called as public key cryptography where individuals are source and destination. The dissimilar keys can be used for encrypting and decrypting purposes. This type of encryption contains SSL, DH, RSA and SSH algorithms [9] and also gets understandable data, jumbles and unscrambles the same at the other end where a dissimilar key is utilized for both the ends. In [10], In order to overcome the cloud security issues, Vijyendra Karpatne and E.J.Thomson Fredrik,2017 proposed Data Protection as a Service (DPaaS) to enhance cloud data security. Their implementation results of DPaaS showed that it eliminated cloud security issues and cloud data integrity issues.

Encoders employ a public key for scrambling data and decoders bring into play the corresponding private key on the other end for unscrambling it. The study of cryptography deals with the procedures for passing on information strongly and its ultimate objective is to permit the anticipated recipients of a message to take delivery safe. A cipher-text is sent out explicitly across a communication channel. Since, it has been encrypted; the nosy people will preferably be unable to discover the significance of the communication. It could be only the deliberated inheritor possessing the suitable key can decrypt the text to pull through the actual text and take the meaning. An asymmetric cipher key employs dissimilar keys for encryption and decryption. Despite being mathematically associated, the keys are very complicated to acquire one from the other unless one recognizes the conversion. The keys used for encryption and decryption are referred as public and private keys respectively. The public key is exposed not negotiating the safety of the system.

III. PROPOSED SYSTEM

Schemes and the domain pointed out in advance have been taken into account in the suggested effort. These mechanisms have been incorporated in the scheme for authenticating and distributing the key. A new protocol has been proposed based on the group intellect which endeavors to accomplish an analogous presentation with the further protocols overcoming disadvantages, scalability, vitality and fortification in opposition to potential threats. MAC is used for authentication during message exchange which speeds up the proposed protocol. Ant colony algorithm has been utilized by this protocol that modifies dynamically ensuring the freshness of the swapped keys and the same has been analyzed using logical tools guaranteeing the attainment of objectives of substantiation and key distribution lacking bugs.

Exploit of predicate routing algorithm puts in security to the network layer by avoiding the nosy human beings. The suggested scheme helps in accomplishing safety measures by all means to the systems. The original key is mediated in the similar mode as public key cryptography. In spite, complexity being the 3rd order, it is implemented only on one occasion where as the input supervision features like generation and MAC are of the 1st order. The procedures brought up earlier have been cautiously utilized making certain that full amount life process of the key management has been attained. The produced outcome and critical analysis of the same has been evidently pictured in the upcoming chapters. The classification is compatibly examined and the hopeful fallouts designate it as an enhanced substitute in the branch of cryptography and network security.

IV. TESTING AND IMPLEMENTATION

The most principal step for testing is the formation time of the keys. The working out point in time for RSA has been realistically lengthy as the procedure absorbs pretty a few exponential and factorizing modular arithmetic functions. Outcomes in progressing effort associating to the key creation are presented in the table 1.1. It explains that, the working out time for generating key in average of RSA algorithm is to a great extent finer to the ACO algorithm and it has been observed to be 5647.5 µsecs while for ACO algorithm it is only 329.44. Furthermore, the existing technique brings into being n2 –n keys making the typical pace improvement in terms of the average computation time which is 16.09365. The Figure 1.1 obviously points out the above observation that, arbitrariness of the time is much elevated in RSA when compared with the existing ACO approach

Iteration	R.S.A in µSeconds	A.C.O in µSeconds
01	13960	442
02	533	392
03	12345	340
04	7743	245
05	5047	345
06	2290	296
07	2739	342
08	525	235
09	6338	244
010	3273	377
011	1469	388
012	5190	340
013	1763	256
014	8283	309
015	8149	421
016	7774	377
017	3652	271
018	3620	296
019	9905	326
020	8349	346

Table 1.1 Seed and Key value comparison

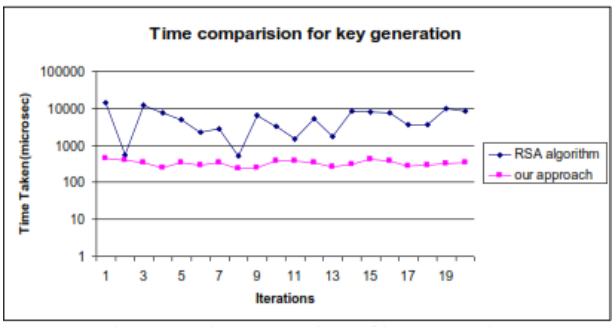

Figure 1.1 Key generation time Comparison

The methodical relation of RSA with Blowfish has been assumed as a piece of modular advance. It is crucial since Public Key Infra Structure is measured to be standard which makes use of the RSA, while the current method utilizes symmetric key approach which is faster to a large extent. The Tables 1.2 and 1.3 correspondingly furnish the encoding and decoding time of RSA and blowfish.

File size	Encryption in µSeconds	Decryption in µSeconds
01	31	1430
02	26	2995
03	41	4420
04	55	5769
05	62	6967
15	109	13621
25	192	26992
55	468	67409
105	860	134385
205	1721	267437
505	4286	670649
1000	8722	1385673

Table 1.2 RSA

File size in Kilo Byte	Encryption time in msec	Decryption time in msec
1	15.07	12.19
2	24.635	11.24
3	17.2	23.89
4	20.5	13.3
5	14.8	14.6
10	26.2	47.3
20	40.6	41.5
50	87.4	69
100	168.2	122.37
200	326.5	262.1
500	818.5	621.2
1000	1735.04	1251.1
2000	3895.7	2930.6

Table 1.3 Blowfish

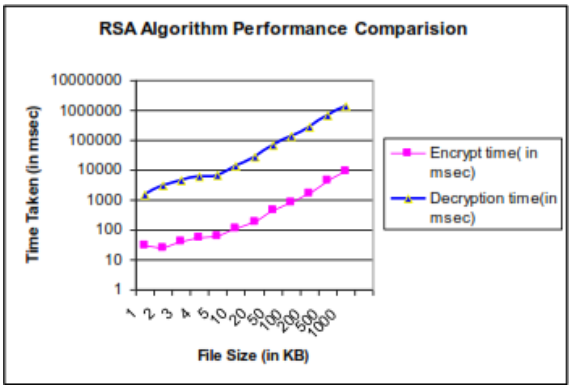

Figure 1.2 Performance Comparisons

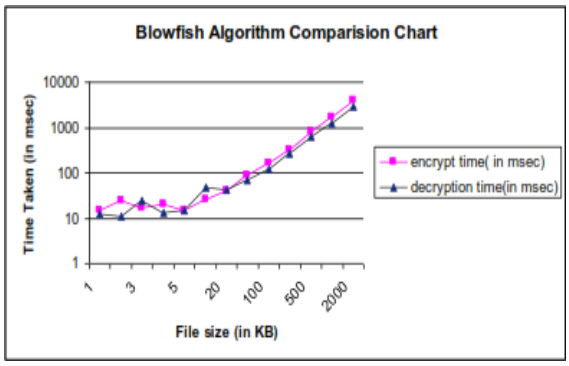

Figure 1.3 Blowfish

The Table 1.2 points out that RSA decryption are 156.2547550 times slower than encryption. These consequences vary in accordance with the file size. It is attractive to note that for a 2 Kilo Byte file it acquires a total of 3018 milliseconds. Decoding / encoding ratio is 117.76 with the first packet used being less than 2Kilo Byte. While comparing blowfish for the equivalent size of the files, it has been observed that the common decoding to encoding ratio is 0.897610365 where encoding and decoding depends only on file size, which points out the development of future method. Blowfish which is compared modularly with RSA also fabricates gorgeous consequences. Encoding using blowfish is on an average 3.907774062 times former than RSA algorithm. The pertinent data has been on hand in table 1.4 and symbolized in figure 1.4

File Size in Kilo Byte	RSA in µSeconds	Blowfish in µSeconds
1	29	15.07
2	24	24.635
3	39	17.2
4	53	20.5
5	60	14.8
10	107	26.2
20	190	40.6
50	466	87.4
100	858	168.2
200	1719	326.5
500	4284	818.5
1000	8720	1735.04

Table 1.4 RSA versus Blow fish

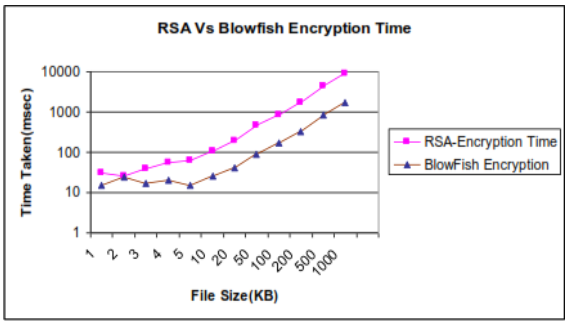

Figure 1.4 Encryption of RSA and Blowfish

The blowfish decoding time has been 641.694989 times faster than RSA. The pertinent data are obtainable in table - 1.5 and represented in the Figure 1.5. A vast dissimilarity in decryption time is owing to the mathematical processes that load the means. Despite RSA is admired and used largely in Public Key Infrastructure, still data safety lies at the stack because of arithmetical solutions and raising the pace of processors. The practice of private key transmission is still anonymous.

Size of the file in Kilo Byte	RSA Decryption in msec	Blowfish Decryption in msec
01	1428	12.18
02	2993	11.23
03	4418	23.88
04	5767	13.2
05	6965	14.5
15	13619	47.2
25	26990	41.4
55	67407	68
105	134383	122.36
205	267435	262.0
505	670647	621.1
1000	1385671	1251.0

Table 1.5 RSA and Blowfish Decryption

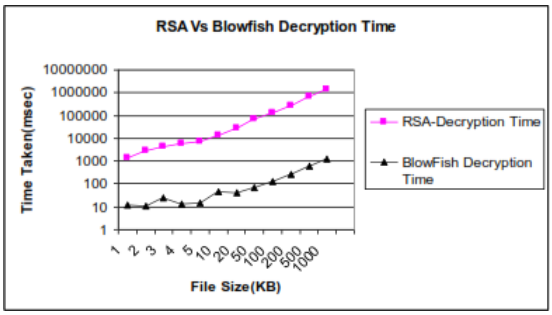

Figure 1.5 RSA and Blowfish Decryption

Hence, Blowfish algorithm which follows the symmetric key cryptographic technique is found to be better than other asymmetric processes which include RSA.

V. CONCLUSION

This paper identifies convinced neighborhood of enhancement which has been pointed out in key administration learning, routing procedure for an enhanced cryptographic appliance. Reproduced results of the recommended method improve the ineffectiveness which has been achieved as accounted up in the later paragraphs. Proposed method is modular and expected to convene the requirements of mounting networks and also has a way out with upgraded competence. This system has also been tested for the communication network which has produced hopeful results. The simulation consequences are in line with the observations.

REFERENCES

[1] Rajesh R Mane A, "Review on Cryptography Algorithms, Attacks and Encryption Tools"; IJIRCCE, Vol. 3, Issue 9, September 2015.

[2] Mrs. Smita Desai, Chetan A. Mudholkar, Rohan Khade, Prashant Chilwant, "Image Encryption and Decryption Using Blowfish Algorithm"; IJEEE, ISSN- 2321-2055 (E),Volume 07, Issue 01, Jan- June 2015.

[3] Anjaneyulu GSGN, Pawan Kumar Kurmi, Rahul Jain, "Image Encryption and Decryption Using BlowfishAlgorithm with Random number Generator"; IJPT, Vol. 6, Issue No.3, 7164-7170, 2014.

[4] Anjula Gupta, Navpreet Kaur Walia, "Cryptography Algorithms: A Review"; IJEDR, Volume 2, Issue 2, ISSN: 2321-9939, 2014.

[5] Ayushi, "A Symmetric Key Cryptographic Algorithm"; International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.

[6] M.Sambasiva Reddy and Mr.Y.Amar Babu, "Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan- 3E", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,

Vol. 2, Issue 7, page 3341-3347, July 2013

[7] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, 2006, Pearson Education, Prantice Hall, ISBN 81- 7758-774 9.

[8] Priya Thakur & Anurag Rana, " A Symmetrical key Cryptography Analysis using Blowfish Algorithm", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 5 Issue 07, July-2016.

[9] Ayushi, "A Symmetric Key Cryptographic Algorithm"; International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.

[10] Vijyendra Karpatne, E.J.Thomson Fredrik, "Enhancing Security of Data in Cloud Environment using Data Protection as a Service (DPaaS)", European Journal of Scientific Research, Vol.147, No.1,September 2017, pp 39-45