ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Data Security in Cloud Computing Via Bio – Inspired Optimization Technique

J.Mahalakshmi[1], K.Kuppusamy[2]

[1] *Ph.D Research Scholar, Department of Computer Science & Engg, Alagappa University, Karaikudi, India*
[2]*Professor, Department of Computer Science & Engg, Alagappa University, Karaikudi, India*

[1]lakshmimsc19@gmail.com, [2]kkdiksamy@yahoo.com

***Abstract*— Cloud computing in distributed computing environment is an emerging technology that offers on-demand service to its users on a pay-as-you-use basis. Numerous resources such as Platform, Software, Infrastructure, and Database are offered by the cloud service providers that seek utmost security. A lot of security mechanisms are in the literature, including cryptographic techniques, service level agreements, accessing policies etc. to secure them. In this paper, a new compound algorithm for data encryption is implemented. It combines the features of logical substitution of improved cipher block chaining algorithm with nature inspired optimization technique for key generation. The algorithm of this encryption technique differs in the way of key generation. A satisfactory level of this algorithm is attained by performing various security and statistical analysis while executing the algorithm. A comparison of this pioneering algorithm is done with existing, industrially accepted algorithms. The Effort of this algorithm is to make the encryption algorithm strengthen and on cryptanalysis process difficult.**

***Keywords*—Encryption Algorithm, Optimization Technique, Cloud Computing, Security Service.**

I. INTRODUCTION

Cloud Computing is a model for enabling on-demand service to the users. Key elements of cloud computing includes the on-demand self service, broad network access, measured service, rapid elasticity and resource pooling [4]. Cloud architecture aims to connect numerous low-cost computing entities into a single system with the capability to distribute computing resources to the end users by various service models [5]. Main goal of cloud computing is to reduce the computation problem and to deliver the resources in rapid manner with utmost security. Hence, our approach tends towards security of the computing resources offered by the cloud delivery models.

In the multi-tenant architecture, securing the data is a major obstacle. Cryptography is a science, using mathematics to encrypt the data. Encryption is the technique of scrambling of data to unreadable format, to protect it from unauthorized access. The encryption falls into two categories as full encryption and partial encryption. Original data is referred as plain text whereas the scrambled data is the cipher text [6]. Lot of algorithms are in state of art to encrypt the data, in which symmetric key encryption is employed for this research work. In the symmetric key encryption a single key is used for both encryption and decryption.

In every cryptographic process, key generation is the important section, which decides the strength of the encryption algorithm. Quandary key problems exists in the literature, has been put to research in recent decades. Now-a-days nature inspired algorithms such as genetic algorithm, ant colony optimization, artificial bee colony, simulated annealing etc are used in the key generation to achieve sub-optimal key to convert the plain text. One of the most specific function genetic algorithm is considered in this research work.

Genetic Algorithm is one among the novel-searching technique filled with superior features designed specifically to work on hybrid algorithm [7]. It is very hard to compute the code of genetic algorithm, also require relatively additional time to compute the optimization problem. Genetic Algorithms are characterized by their robustness as well as their ability to deal with non-convex problems in dynamic environment [8]. Cryptanalysis is the art and science of analysing information systems in order to study the hidden aspects of the systems. Mathematical analyses are used to study the effect of attacks taken place in the transmission medium [3].

Our Contribution

Data security at the data centres is the prominent issue consider in this paper. Many cases, it is the work of the provider to guarantee that their infrastructure is secure enough via implementing access policies and security mechanisms. The algorithm introduced in this paper, simultaneously works

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

on chunks of data, involves substitution operation as well as involves Genetic Algorithm for key generation. Together this algorithm remains difficult to encode and encryption quality is increased.

Rest of the paper is constructed as follows. Section 1 briefly discussed on basic introduction about symmetric key encryption and Genetic algorithm. Section 2 contains related works regarding this proposed encryption algorithm. Section 3, elaborately defines the proposed encryption algorithm, key scheme. The analysis regarding the performance of the proposed algorithm is reported in Section 4. Section 5, poses some concluding remarks about this research work.

II. RELATED WORK

Manas Paul and Jyotsna Kumar Mandal [9], proposed a technique that is very secure and suitable for encryption of large files of any type. Session Based Symmetric Key cryptographic Technique (SBSKCT), that considers the plain text as a string with finite number of binary bits. This input binary string is broken down into blocks of various sizes. The encrypted binary string is formed by shifting the bit position of each block by a certain values for a certain number of times and from this string cipher text is formed. With the help of session key information the binary string is broken down into blocks and decrypted using bit shifting method. Comparisons of their algorithm, with existing algorithms have done by the authors.

Satyajeet R. Shinge and Rahul Patil [10], explained the encryption algorithm based on ASCII characters. The algorithm given by the author encrypts the plaintext using their ASCII values. The secret key is converted to another string and is used to encrypt or decrypt the data. It provides good results against time complexity. It took less execution time when the ASCII converted string is used for the encryption process. Makhlouf Hadji [11], explained on the scalable algorithm used for the reliable cloud computing. The author presented two algorithms, to place cipher data at blocks as well as to minimize the cost of storage. The algorithm of the author is based on b-Matching and Commodity Flow theory to optimize the storage cost and the network latency.

M.S. Ismail et.al., [7], reported on the use of Genetic Algorithm to produce optimized modeling of hybrid energy systems. According to the authors GA is one among the optimization technique that remains with special features to compute in hybrid environments. The ultimate aim is to reduce the cost of the system. S.G.Srikantaswamy and H.D.Phaneendra [6], explained the Cryptosystem Design with Recursive Key Generation Technique, combine the feature of both substitution and transposition. About five different keys were used by the authors for the encryption purpose. Left shifting is done for transposition.

Satyajeet R. Shinge , Rahul Patil [12], explained the encryption algorithm based on ASCII characters. The algorithm given by the authors encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data. It provides good results against time complexity. It took less execution time when the ASCII converted string is used for the encryption process.

Vaidehi, M. and Rabi, B.J [13],experimentally verified the Design and analysis of AES-CBC mode for high security applications. From their results it is clear that the, more complex modes of operation combine the data of the previous ciphered blocks and use Initialization Vectors (IV) to make each ciphered message unique. The AES Cipher-Block Chaining (CBC) mode includes these features. Before encrypting a block, it is XORed with the cipher text of the previous cipher text block. The design and analysis of AES-CBC mode is presented by the authors to find the fault during the encryption process. Simulation is performed to analyze the chip size reduction.

Padhmavathi, et al. [14], have explained on the Cipher Block Chaining encryption method by using the Merkle-Hellman Knapsack Cryptosystem that allows, only the authenticated receiver of the message to decipher the message. Xinxian Li et.al [15], reported the use of private cloud file encryption methodology with the aid of tripartite secret key protocol. A certificate less encryption algorithm is recommended by the authors which yields better results for large scale environment. Despite the limitations results made by the authors reveals that the files are communicated with high security.

The literature review shows the use of various modes of operations that will yield better security to the blocks of data. The AES, one of the strongest encryption algorithm is widely used to encrypt the text data. The logical operators, especially the XOR operator is the self invertible operator, hence the decryption is easier. The ASCII conversion of data makes it more flexible and increases the speed of processing. The key generation from the genetic algorithm proves the quality enhancement and strength of the proposed encryption algorithm. Therefore, in this paper a new algorithm that combines the substitution mode, logical operators as well as the optimization technique is proposed to enhance the encryption process and the experimental results yields better results.

III. PROPOSED ENCRYPTION ALGORITHM

This section provides basic information about structure format that was used in implementation process. The given input plain text is converted to its corresponding ASCII [American Standard Code for Information Interchange] character. Again, conversion of binary to consequent ASCII Character is taken place. Let us assume that the input data as

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Matrix blocks. If M is a matrix, then M_{nm} is a 8 X 8 matrix, whose elements where represented using 8 bit binary structure, where m,n indicates the elements in the matrix. After, the conversion, Key generation process follows. The proposed Encryption algorithm consists of three major components: Encryption, key generation and Decryption process. This algorithm involves usage of various logical operators, for the input text, that converts input into unintelligible format.

A. Key Generation Process

In any cryptographic process key generation is most significant part. In this proposed algorithm key generation takes place in three stages. The first key generation is in binary format. The resultant matrix from the encryption process is taken as input. It is now passed through the cipher block chaining operation mode. Set the Initialization vector (IV) with 8-bit binary input. Assume that X_i is the initial 8-bit of the block matrix and Y_i be the Initialization vector. Then, the resultant output is X_i XOR Y_i. The output value is again fed as input to the next 8 – bit input value and the process is repeated till end of the file matrix is reached. The resultant matrix is the matrix with converted plain text to cipher.

The second key matrix generation is taken place. It is also taken as 8 x 8 block matrix. The binary bits are taken from the pseudorandom generators. The resultant ciphered matrix is now Exclusive disjunct with the key matrix generated. The output is the 8 x 8 matrix, whose elements are completely ciphered. Repeat the process, until end of file is reached. The result code is encoded to ASCII character set. Now, the text file is completely encrypted.

Genetic algorithm is employed for this proposed algorithm, with aim to minimize the execution speed. Final as well as sub-optimal key is evolved as a result of four steps. This nature inspired algorithm is one among the direct approach that utilizes a precise objective function, to locate either the minimum or the minimum. The key generation is as follows,

- *Population*: The mathematical model consists of the entire data, from which the key is to be generated.
- *Selection*: Choose some bits in random so as to construct the sub-optimal key. The fitness function is evaluated and main constituent matrix to perform cross over is selected.
- *Crossover*: Matrix block of size 8 x 8 are cross overed and as a result two new offspring's are generated.
- *Mutation*: Between the pair of generated offspring's, mutation operation is performed. The fitness function is again calculated for this new offspring's to achieve the optimized results.

As soon as, on exact arrival of the fitness function, from multiple iterations, the process stops and the new sub-optimal key is produced. This key is again XORed with the encoded matrix to attain complete encryption.

B. Encryption Process

The compound model of logical substitution operations along with the sub-optimal key generation makes the cryptographic process as a new encryption method. The logical Exclusive Disjunction operator (XOR) is used for the substitution process, since it is self-invertible. The cipher block chaining encryption operation mode is involved where the blocks are operated at chunks. The output matrix thus generated is completely ciphered.

C. Decryption Process

The decryption is the reverse of encryption process. The deciphered output matrix is fed as input and key generation steps taken place. Finally, the binary strings of original input are left out, which is converted to corresponding ASCII values. The Key generation process is complex to compute, because of the multiple key generations involved for the process in parallel. Hence, when number of keys is increased the encryption code automatically strengthened.

IV. RESULTS AND DISCUSSIONS

A. Security Analysis

The proposed method is implemented with Visual Studio 2010, C# language under the configuration of windows 7 operating system with Core-i3 and 3 GB RAM. This section presents the results and outcomes from the proposed Encryption algorithm. This includes the encryption time and decryption time for every input series. A security analysis for the algorithm is also given by measuring the execution time parameters. Finally, the results for the proposed algorithm are explained. The algorithm is implemented on notepad files with various file sizes to verify the efficiency of the algorithm.

Table I shows the encryption time and decryption time for proposed algorithm for various file size such as against the different files. Proposed algorithm takes very less time to encrypt/decrypt than Existing and little bit more time than AES. The measurement was taken place in seconds. For the numeric characters and the alphanumeric characters the algorithm takes minimum time seconds to encrypt.

TABLE I. TABLE WITH TYPE OF CONTENTS IN FILE AND THE TIME TAKEN IN SECONDS

Type of Characters	Seconds
Alphabets in Lower Case	0.0026
Alphabets in Upper Case	0.0027
Special Characters	0.0020
Numeric Characters	0.0010
Alphanumeric	0.0019

B. Comparative Analysis

In this section a comparison is done between the proposed encryption algorithms to that of the existing algorithms. Difference in the encryption and decryption time between

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

the methods is listed in the following table 2. Experimental results have been conducted for varied type of characters for the text files. The authors on Ref [1] made an advanced encryption algorithm that is capable of work more securely than the algorithm of Ref [2], DJSA algorithm. The author in the Ref [3], plots the time taken to encrypt the data, which is larger than the proposed algorithm. The figure 1 depicts the time difference in seconds between various methods. The proposed encryption algorithm executes in less timing, thus reducing time complexity for encryption.

TABLE II. COMPARISON ON ENCRYPTION TIME DIFFERENCE IN SECONDS

Plain Text Size	Extended MSA – DJSA Algorithm [Ref -2]	Advanced Encryption Algorithm [Ref - 1]	Block Cipher Based Cryptographic Method [Ref – 3]	Proposed Method
560kb	3.7 Secs	2.8 Secs	1.3 Secs	3.4 Secs
187 kb	1.8 Secs	9.0 Secs	5.0 Secs	1.8 Secs
16kb	1.0 Secs	1.0 Secs	2.0 Secs	0.6 Secs

The existing algorithm DJSA, used the symmetric key encryption, for which key is generated from random number generators followed by basic substitution method. Replacement process between the bit blocks is taken over in the DJSA algorithm. The authors of the Advanced Encryption algorithm use the logical operation as well as the shifting of bit blocks.

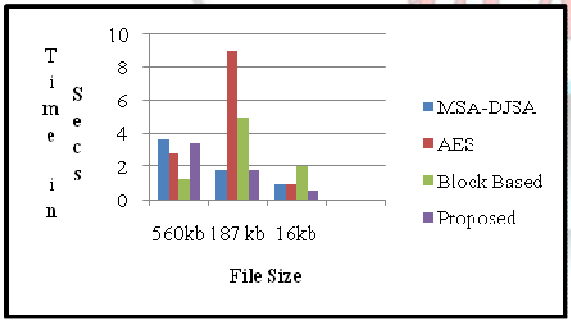

Fig 1. Chart Displays Time Difference in Seconds.

V. CONCLUSION

A compound encryption algorithm for data encryption has been proposed in this research work to reduce the time and space complexity. To strengthen the key employed for encryption three techniques were involved: improved cipher block chaining, pseudorandom number generator and the biological based genetic algorithm that produces optimized key from large set of population. Narrated experimental results confirm the computational efficiency of the proposed algorithm via minimizing the encryption and decryption time. The results of the statistical and security analyses in this paper, indicates the efficacy of the algorithm. The main aim of this research work is multi-objective; one is to reduce the time for encryption and another to reduce the storage space. Both the objectives are attained by this hybrid algorithm. Comparative analysis shows the potential of the algorithm.

ACKNOWLEDGMENT

The author expresses deep sense of gratitude to the Alagappa University, Karaikudi, India for the financial assistance through Alagappa University Research Fellowship - Grant No. Ph.D / 0833 / AURF Fellowship / 2015, to carry out this research work.

REFERENCES

[1] Viswa Gupta, Gajendra Singh and Ravindra Gupta. “Advanced Cryptographic Algorithm to improve data security”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, pp 1-6, January 2012.

[2] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath. “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” International Conference on Communication Systems and Network Technologies, IEEE, 2011.

[3] J.Mahalakshmi and K.Kuppusamy ,"A Block Cipher based Cryptographic Algorithm to enhance the Data Security", in International Journal of Applied Engineering Research, Vol. 10, No. 55, 2015,pp:1866-1870.

[4] Tharam Dillon and Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", in 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp:27-33.

[5] GaiZhen Yang, Zemin Zhu and Fen Zhou, " The Application of Saas-based Cloud Computing in the University Research and Teaching Platform", in 011 International Conference on Intelligence Science and Information Engineering, pp:210-213.

[6] S.G.Srikantaswamy and H.D.Phaneendra, " A Cryptosystem Design with Recursive Key Generation Techniques", in Procedia Engineering, Vol. 30, 2012, pp:170-173.

[7] M.S. Ismaila, M. Moghavvemi and T.M.I. Mahlia, "Genetic algorithm based optimization on modeling and design of hybrid renewable energy systems", in Energy Conversion and Management, Elsevier, Vol. 85, 2014,pp: 120–130.

[8] Juan P. Fossati, Ainhoa Galarza, Ander Martín-Villate, José M. Echeverría, Luis Fontán, "Optimal scheduling of a microgrid with a fuzzy logic controlled storage system", in Electrical Power and Energy Systems, vol. 68, 2015,pp: 61–70.

[9] Manas Paul and Jyotsna Kumar Mandal (2012),” A Universal Session Based Bit Level Symmetric Key Cryptographic Technique to Enhance the Information Security”, in International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July pp:123 – 136.

[10] Satyajeet R. Shinge, Rahul Patil, (2014), “An Encryption Algorithm Based on ASCII Value of Data”, in International Journal of Computer Science and Information Technologies, Vol. 5, No. 6 , pp: 7232-7234.

[11] MakhloufHadji, "Scalable andCost-Efficient Algorithms for Reliable and Distributed Cloud Storage", in Springer International Publishing Switzerland 2016, CCIS 581, pp. 15–37, 2016.

[12] Satyajeet R. Shinge, Rahul Patil, (2014), “An Encryption Algorithm Based on ASCII Value of Data”, in International Journal of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Computer Science and Information Technologies, Vol. 5, No. 6 , pp: 7232-7234.

[13] Vaidehi, M. ,Rabi, B.J (2014), "Design and analysis of AES-CBC mode for high security applications", in current trends in engineering and technology 2014 2nd international conference, pp 499-502.

[14] Padhmavathi, B., Ray, Arghya, Anjum, Alisha, Bhat, Santhoshi, 2013. Improvement of CBC encryption technique by using the Merkle-Hellman Knapsack Cryptosystem. In Intelligent systems and controls (ISCO) , 7th International conference, 340-344.

[15] Xinxian Li, Weiqin Li and Daisong Shi, 2015. Enterprise private cloud file encryption system based on tripartite secret key protocol. In International Industrial Informatics and Computer Engineering Conference, Published by Atlantis Press, 166-169.