DOI: https://doi.org/10.24113/ijoscience.v3i9.20

Bio Inspired Algorithm for Secure Cloud Storage: A Review

Ms. Mona Vishwakarma
M.Tech. Scholar
Department of CSE
NRI
Bhopal, M.P., India
shrma.meenu65@gmail.com

Mr. Umesh Lilhore
Professor
Department of CSE
NRI
Bhopal, M.P., India
umeshlilhore@gmail.com

***Abstract* - Cloud storage is one among the service provided by Cloud computing within which information is maintained, managed, secured remotely and created available to users over a network. Now a day's cloud computing is being used in several areas like industry, medical, science and research, colleges etc for storage of huge amount of data. User can retrieve data files from cloud data center on request. While storing data files on cloud server several security issues may arise. To overcome from these security issues there are a number of techniques. Out of several security techniques Cryptography is more popular now a day's for data security. Use of a traditional cryptography algorithm is not effective or sufficient for high level security to data in cloud computing. In this research work a study is presented for bio inspired cryptography technique. The SaaS (software as a service) demonstrates the security using the upload, download and sharing of files using the bio-inspired platform.**

Keywords - Cloud Computing, Security, Confidentiality, Authentication, Bio-inspired algorithms, Genetic Algorithm, DNA Sequencing.

I. INTRODUCTION

Cloud computing is new generation technology; a number of applications are developed now in these days using the cloud platform. Among them social media, banking solutions, ecommerce solutions are played more important role in this era. All of these applications are developed in order to serve continuously without any complexity. Therefore these applications are hosted with the cloud platforms. The main reason behind this, the cloud offers scalable storage and computing solutions. But such kind of applications is requiring some sensitive and private information. Additionally leakage of information and data can make trouble for the organization and also for the end user. In this context the security is an essential concern in the cloud computing and storage [1].

Cloud computing aims at providing on-demand, reliable, and customized services to the customers. Cloud computing provides computing services that is, both hardware and software services to the customers on-demand through the network irrespective of the platform used and location. It is a pay-as- per-use model, where the users pay only for the computing power utilized, without incurring the initial setup expenditures [2, 3].

The proposed work is dedicated to study about the security and privacy issues of the cloud during the data exchange amount client and server. In order to provide security most of the cloud service provides utilizes different security techniques for securing information during data exchange. Among them the cryptographic techniques are widely accepted technique. The main reason for utilizing the cryptographic technique for security is their simplicity and low cost implementation.

II. BIO INSPIRED SECURITY MECHANISM

Cloud computing is an answer of new generation computational and storage requirements. Now in these days every application are designed in such manner by which more and more traffic is collected using the applications. In addition of that the reliable and long term services are also deployed using the SaaS (software as a service) concepts [1]. The key reason behind development of SaaS, these applications are never compromises with the performance of applications additionally the cloud platform provides a secure and scalable storage solutions for the applications [2, 4]. Among them the ecommerce, social sites and the banking applications are frequently utilized SaaS platforms. In this applications sometimes private and confidential information are also communicated, such as credit card information, banking credentials or the organizational emails. Leakage on such kind of data can affect the end client. Thus in this presented work the cloud security and channel security is the main to improve. Therefore various security techniques are studied and found that the cryptographic techniques are providing the security for the communicated data.

In the recent times the biologically phenomenon have provided solutions to many computational problems. This area of research is called as Biologically Inspired Computing(BIC). Apart from the standard cryptographic algorithms, there has been research in the area of biologically inspired algorithms which are applied into the area of cryptography. Biological systems are complex systems which are capable of processing complex information and are capable of providing solutions to many problems in engineering and technology. Modern artificial systems are mostly based on the biological phenomenon and systems like neural networks, immune systems, genetic behaviors etc [5]. BIC paradigms which are applied in the field of cryptography are categorized into: Genetic Algorithm(GA), Artificial Immune System(AIS), DNA, Cellular Automata (CA), Artificial Neural Networks(ANN), and Ant Colony Optimization(ACO). The above mentioned methodologies are explained in detail below.

A. Artificial Neural Network

Artificial Neural Networks (ANN) model depicts how the computations happen inside the human brain. This model contains large number of hugely interconnected processors namely neurons, which depict the biological neurons in the brain. Neurons are connected by weighted links for communication between them.

As it is a huge interconnected network of neurons, the flow of information between them defines the network model. ANN is known for their learning ability. There are two types of learning-supervised and unsupervised. Applications of ANN in cryptology is divided into two sub divisions one is key management and the other is cryptanalysis. Neural key exchange mechanism is relatively a new research area. The neural key exchange is based on the synchronization between the neurons by mutual learning. Jagadeeswari et al. [4] proposed a model which is a combination of dynamic hashing fragmented component for data confidentiality and neural data security model for encryption and decryption of data.

Negi et al.[5] proposed a security framework to enhance security for cloud computing using ANN. The model proposed mainly consists of two phases. One is authentication phase using symmetric key process and second phase to ensure only the authenticate user can send or receive data. The author proposes the model inspired by counter propagation neural network.

B. Artificial Immune System

Artificial Immune System(AIS) which is inspired by the human immune system(HIS) is a fast growing field in the domain of computational sciences. It provides robust solutions to complex information processing problems. The basic functionality of the immune system is to provide protection against foreign cells and remove the damaged and nonfunctional cells. Artificial Immune Systems have immensely contributed to the field of cryptography and cryptanalysis. AIS has the ability to act as a anomaly detection system which can detect week and fake ciphertext from the honest ones. In this system, key generation algorithm and the ciphertext are the inputs and the output is the cryptanalysis report.

Phangal et al.[6] had proposed a data security strategy based on Artificial Immune Algorithm. According to the model, negative selection was selected to mature antibodies by then files stored in data node could be detected and arranged in optimized node. New files were created and manage into a data node based on the clone selection algorithm.

C. Genetic Algorithm

Major works that focus on genetic algorithm are usually done for the crypt-analysis on usual ciphers. A lot of work is done in this domain, few of them are mentioned in this section.

Clark[3] had performed extensive research in cryptanalytic attacks. He proposed many attacks on classic ciphers. He even proposed a parallel genetic algorithm for attacking the polyalphabetic substitution cipher by attacking each of the key positions simultaneously. The fitness function used was based on phi test for non-randomness of text.

Naik et al.[8] had proposed an asymmetric key encryption algorithm which was designed using the bio-inspired genetic algorithm. Genetic algorithm is generically used for solving the optimization problem as it provides robustness. Here the genetic algorithm is applied for the cryptographic domain. The basic advantage of genetic algorithm is that it does not break with any change in the inputs. In this paper, the authors have utilized the crossover and mutation functions of the genetic algorithm for the generation of the key pair for the encryption and the decryption algorithms. The length of the secret key is determined by the number of crossover points, mutation points along wit the random byte and permutation factor. So as to maintain uniformity, each parameter is represented using 4 bits. The size of the key generated is 36 bits.The strength of the algorithm is the permutation of the asymmetric key, and the number of permutations is agreed upon by both the sender and the receiver. Authors of the paper claim that, this randomness makes the algorithm robust.

At first Spillman et al.[7] had applied genetic algorithm in crypt-analysis to analyze simple substitution ciphers. In his work he even specified that genetic algorithm can also be used to cryptanalyse knapsack ciphers. He derived his fitness function using single character and diagram frequency distribution.

N. Hitaswi et al. [10] proposed a genetic algorithm based security mechanism. The proposed model utilizes the properties of attribute-based encryption for the key generation and management. The proposed methodology is more suitable for the cloud scenario, as it takes less execution time thereby decreasing the latency and increasing the performance of cloud.

D. DNA Cryptographic Algorithm

The technique is a substitution based technique that transforms the entire text message into the AGTC encoding. This algorithm promises to provide enhance security with less amount of resource consumption. Therefore in order to improve the communication security the DNA cryptographic algorithm is implemented with the cloud service.

Phangal et al.[6] proposed an approach which is an improvement over the traditional symmetric key encryption algorithms. This approach is inspired by the concept of DNA sequencing. DNA sequencing is considered as an input key to the model and DNA substitution is used for cryptography and applied to images. The key generation algorithm in this model uses the DNA sequences. Ranalkar and Phulpagar[17] proposed a security model for data security in multi cloud. It uses a DNA based cryptographic algorithm to provide data hiding in cloud environment. Data in this model is DNA encrypted using two principles- binary coding rule and complementary rule. Then data hiding is done by embedding the cipher text generated into the DNA sequence.

Abbasy and Shanmugan[1] proposed a data hiding mechanism to hide data in DNA sequences, there buy increasing the confidentiality and complexity in cloud environments. There exists many more authors who have contributed in the field of DNA cryptography and continuous research is going on in the particular domain.

Shruti Goyal et al. [11] presented a work based on DNA cryptographic algorithm for security. The DNA based cryptographic technique is basically developed using the substitution and other basic operator's implementation. Thus this technique is less computational cost effective and efficient.

III. DNA CRYPTOGRAPHY

In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1. But DNA digital coding can be encoded by four kind of base that is ADENINE (A) and THYMINE (T) or CYTOSINE (C) and GUANINE (G). There are possibly 4!=24 pattern by encoding format.

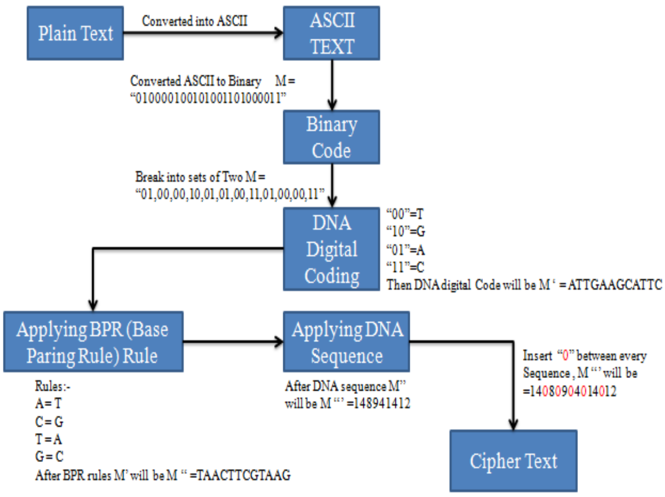
Plain Text
Converted into ASCII
ASCII TEXT
Converted ASCII to Binary M = "010000100101001101000011"
Binary Code
Break into sets of Two M = "01,00,00,10,01,01,00,11,01,00,00,11"
DNA Digital Coding
"00"=T
"10"=G
"01"=A
"11"=C
Then DNA digital Code will be M ' = ATTGAAGCATTC
Applying BPR (Base Paring Rule) Rule
Rules:-
A = T
C = G
T = A
G = C
After BPR rules M' will be M " =TAACTTCGTAAG
Applying DNA Sequence
After DNA sequence M" will be M "' =148941412
Insert "0" between every Sequence , M "' will be =14080904014012
Cipher Text

Figure 1: DNA Encoding Process

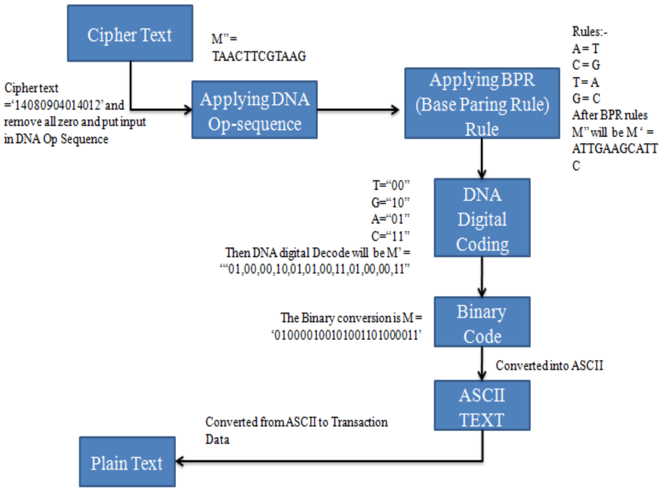
Cipher Text
M"= TAACTTCGTAAG
Cipher text ='14080904014012' and remove all zero and put input in DNA Op Sequence
Applying DNA Op-sequence
Applying BPR (Base Paring Rule) Rule
Rules:-
A = T
C = G
T = A
G = C
After BPR rules M" will be M ' = ATTGAAGCATT C
T="00"
G="10"
A="01"
C="11"
Then DNA digital Decode will be M' = ""01,00,00,10,01,01,00,11,01,00,00,11"
DNA Digital Coding
The Binary conversion is M = '010000100101001101000011'
Binary Code
Converted into ASCII
ASCII TEXT
Converted from ASCII to Transaction Data
Plain Text

Figure 2: DNA Decoding Process

Here in this algorithm, ATGC is being used as a key. Every bit have 2 bits like A=00, T=01, G=10, and C=11 and by using ATGC, key combinations is generated and give numbering respectively. To understand the scenario of proposed DNA cryptography flow chart is illustrated in figure 1. DNA decoding process as shown in Figure 2.

IV. CONCLUSION

Cloud computing is a new generation technology. That is becomes more and more popular as the new and traditional end clients are increasing for their personal and professional use. The main reason behind this popularity is their efficient and scalable computing and storage solutions. According to the needs of applications the cloud offers storage and computing resources on demand. Thus the applications are also becomes more and more effective and efficient. Due to this a significant amount of new applications are deployed on cloud servers among some of them are utilizes the personal and confidential information of the end user. Additionally these online cloud service are accessible in public networks, thus security is key concern in such open communication. Due to this a cryptographic security is proposed for implementation. The proposed work is intended to develop a SaaS (software as a service) for providing the secure communication over the cloud data storage. Therefore to secure the communication an available bio-inspired based cryptographic technique is adopted and integrated. The implemented system offers security during communication among client and server. In addition of that it also offers security during storage of data over cloud. The main aim of this study is to find secure communication using the DNA cryptography for cloud platform is achieved successfully. In near future the following extension is possible for the proposed concept.

REFERENCES

[1] Abbasy, M. R. and Shanmugam, B, Enabling data hiding for resource sharing in cloud computing environments based on dna sequences. In 2011 IEEE World Congress on Services, pages 385390. IEEE,2011.

[2] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I, Cloud com- puting and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6):599616, 2009.

[3] Clark, A. J. (1998). Optimisation heuristics for cryptology.60 Dimovski, A. and Gligoroski, D., Attacks on the transposition ciphers using optimization heuristics. In International Scientific Conference on Information, Communication & Energy Systems & Technologies ICEST, 2003.

[4] Jegadeeswari, S., Dinadayalan, P., and Gnanambigai, Enhanced data security using neural network in cloud environment. International Journal of Applied Engineering Research, 11(1):278285, 2016.

[5] Negi, A., Singh, M., and Kumar, S, An efficent security framework design for cloud computing using artificial neural networks. International Journal of Computer Applications, 129(4):1721, 2015.

[6] Phangal, S. and Kumar, M, A dual security scheme using dna key based dna cryptography. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 37. ACM, 2014.

[7] Spillman, R., Janssen, M., Nelson, B., and Kepner, M., Use of a genetic algo- rithm in the cryptanalysis of simple substitution ciphers. Cryptologia, 17(1):3144, 1993.

[8] Naik, P. G. and Naik, G. R, Symmetric key encryption using genetic algorithm. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3(3):118128,2014.

[9] Ranalkar, R. and Phulpagar, B, Dna based cryptography in multi-cloud: Security strategy and analysis. pages 189192, 2014.

[10] N. Hitaswi and K. Chandrasekaran, “A Bio-Inspired Model to Provide Data Security in Cloud Storage”, IEEE, 2016.

[11] Shruti Goyal, Sourabh Jain, “A secure cryptographic cloud communication using DNA cryptographic technique”, ICICT, IEEE, 2016.