iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VII **Month of publication:** July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7054

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Review Paper on Security of Cloud Computing using Genetic Algorithm

Shivani[1], Rajnish Kansal[2]
[1]*M.Tech Student,* [2]*Assistant Professor, CSE, Asra College of Engineering and Technology, Bhawanigarh, Punjab, India*

Abstract: ***This paper is a review paper of security of cloud computing using genetic algorithm. As cloud has become very popular these days, every organization, every institute, company and even individual person is using cloud to store their data in managed and secure way. So, security of cloud becomes a critical issue. Here, a different method which is proposed to secure the cloud data is reviewed. It uses genetic algorithm to secure the data rather than using cryptography algorithms where keys are as important as data. In the proposed method, two genetic operations, crossover and mutation are applied for the purpose of encryption and decryption on the blocks of data. When the genetic algorithm is applied on blocks of bits it creates ciphertext, ciphertext is stored on distinct location on the cloud. Therefore, it will be very difficult to detect the location of the ciphertext for the attacker.***

Keywords: Genetic algorithm, cloud security, cryptography, crossover, mutation, ciphertext.

I. INTRODUCTION

Cloud computing provides on demand services to users. Users have to pay only for what they use. It provides the resources online to share and use. Cloud computing has many advantages like resource pooling, enhanced collaboration, manageability, cost effective, pay-per-use, reliability, scalability, flexibility, on-demand self service and many more. Cloud service provider hosts the data of data owner at their servers. Data owners do not store the data at its own side because it may not be cost effective; it can be theft, breached, destroyed or crashed at any time but stored at cloud service providers. Cloud service providers store the data at data centres at distinct locations and multiple locations as backup so that if some data is lost or destroyed it can be recovered from there. So security of cloud is very crucial. Many researchers have worked on it, working, and provided the solutions for this. Most of them suggested cryptography methods and techniques which using key concept. The big issue with the key concept is the trust between two parties that share the key. It means the key is as important as the data to be secured. Here, the proposed method uses the genetic algorithm operations for encryption and decryption process. Two genetic operations are used here i.e. crossover and mutation. The proposed method ensures data security and confidentiality.

II. PROPOSED METHOD

In this new security framework, the data owner receives the data from the user and then proposed method is implemented upon it. Data is converted into ASCII values. Then these ASCII values are converted into binary bits. Binary bits then divided into blocks of bits of some size. Block size taken here is of 8 bits. Two Genetic algorithm (GA) operations (crossover and mutation) and pseudorandom number is used. The GA operations for encryption and decryption process are used in this proposed system. These operations are applied on each pair of blocks. The final output of each GA operations is a ciphertext which will be stored at distinct locations by some mechanism at cloud so that cloud service provider cannot see the data. These encrypted data parts are further encrypted with private key of Data owner, then encrypt the encrypted data is again encrypted with public key of CSP again so that attacker can't see the data and CPList. Then the data is sent into cloud service provider.

A. Perform The Following Operations On The Block Of Bits

1) Generate pseudorandom number using pseudo random number generator. It is multiplicative congruential generator. The function xi+1= xi.c (modulo m) is used to generate pseudo random number; where xi+1 is the Pseudo Random Number(PRN) of x i, c and m are positive integer numbers, c is frequently multiply by xi and the outcome is xi.a and it is divided by m. As far as the remainder comes less than m.x0 is the first number by which, it starts calculating the PRN. Here, the new number is generated from previous one. Output of modulo operation on generated pseudo number decides which crossover operation should apply on two selected blocks of data.

2) Then apply Crossover genetic operation. It is decided by pseudorandom number which crossover operation to apply.It is the process in which two blocks are taken to generate a new offspring. There are mainly three crossover operations which are used on binary coded GA; one point crossover, two point crossover and uniform crossover.

3) Mutation, it is based on random changes; it changes 0 to 1 and vice versa. It is performed on two selected chromosomes or blocks.

B. Steps for User

1) Firstly, the user get registered himself by following the registration request to data owner with his details. Data owner gets connected with the Cloud Service Provider and send all the user details using user registration process algorithm. The user will be provided the details.

2) By applying split algorithm, data is converted into ASCII values, apply genetic operations for encryption process and store the encrypted data on cloud at distinct locations.

3) If the user wants to access the data, the request will be sent to cloud service provider along with his details for authentication, then cloud service provider fetches the data, the user will download the decrypted data.

4) All the user details are stored in capability list.

III. IMPLEMENTATION

The proposed method is implemented in visual studio tool using C# language. There are different pages and modules for user registration, login, encryption, decryption and download files. If the user is new user, he must have to register first by filling his details like username, password, contact number, email id as shown in Figure 1. After successful registration he will be allowed to send the data for the implementation of the proposed method. The existing users just have to fill username and password to get login as shown in Figure 2. There are different options available to encrypt the file, download, zip file, steganography and sign out as shown in Figure 3.

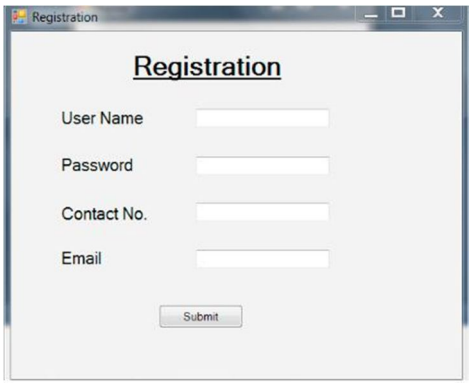


Figure 1: New User Registration

Figure 2: Existing User Login

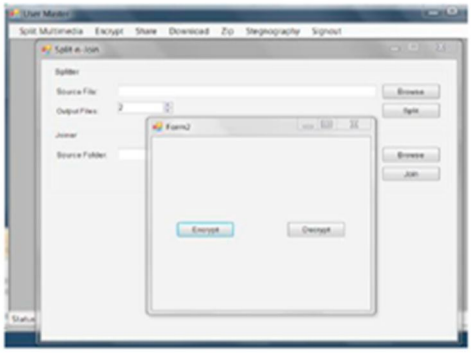


Figure 3: All options

IV. RESULTS AND DISCUSSION

Here, the genetic algorithm which is adaptive heuristic search algorithm is used in a unique way. This paper is the review paper which is having previous paper concept. This scheme can further be extended by focusing at the schedule of task. Also, it will be time effective if data is classified first into most important, moderate and least important data before the implementation of proposed scheme. This scheme has no key concept as it uses genetic operations for encryption and decryption process. The ciphertext which is generated is stored at distinct locations so that attacker can never find where the data is and at multiple locations for backup. The user has to do registration first and then only the user can login into the system. There are different options available to apply. It ensures data security and confidentiality.

V. CONCLUSION

In the proposed method, genetic operations are applied on the small blocks of bits. It ensures security of data. Here, block size is of 8 bits. If block size is taken of lesser size then the number of genetic operations will also increase. The ciphertext corresponding to data bits also have more number of random bits. Therefore, confidentiality of data increases as randomness of data increases. The data owner sends the data to cloud service provider after encryption. Only the authentic and registered users are allowed to access the system by filling their details like username and password to login after registration.

REFERENCES

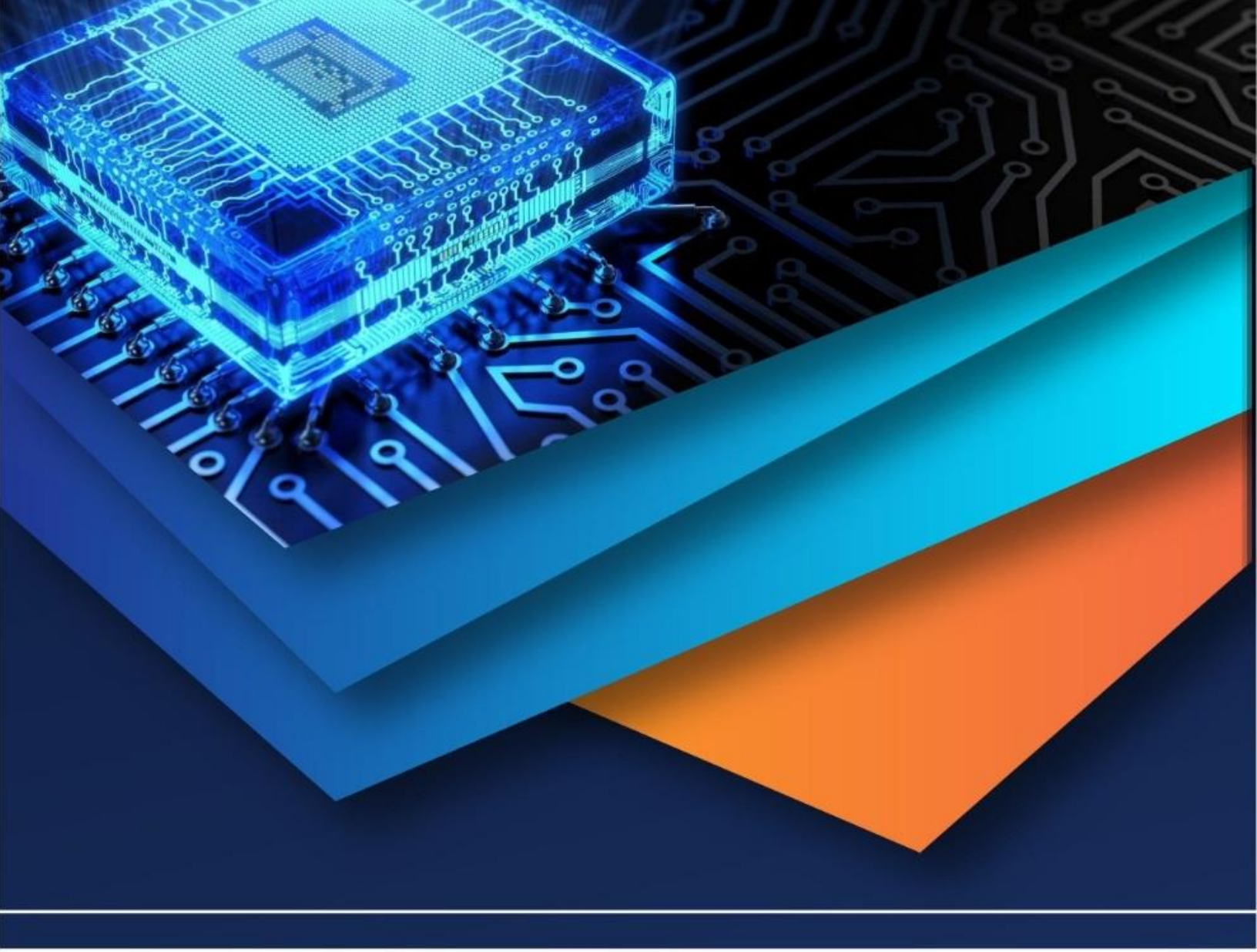
[1] A Venkatesh, Marrynal S Eastaff, “A Study of Data Storage Security Issues in Cloud Computing”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3 | Issue 1 | ISSN : 2456-3307, 2018 IJSRCSEIT

[2] Acqueela G Palathinga, Anmy George, Blessy Ann Thomas, Ann Rija Paul, “Enhanced Cloud Data Security using Combined Encryption and Steganography”, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03 | Mar-2018

[3] Nabeel Khan, Adil Al-Yasiri, “Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework”, The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies(IoTNAT’ 2016)

[4] Safwat A. Hamad, Fatma A. Omara, “Genetic-Based Task Scheduling Algorithm in Cloud”, 5(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016

[5] ShaluMall, Sushil Kumar Saroj, “A New Security Framework for Cloud Data”, 8th International Conference on Advances in Computing and Communication (ICACC-2018)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY