iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XI **Month of publication:** November 2019

DOI: http://doi.org/10.22214/ijraset.2019.11004

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 XI, Nov 2019- Available at www.ijraset.com

Security of Cloud Computing using Genetic Algorithm

Shivani[1], Rajnish Kansal[2]
[1]*Mtech Student,* [2]*Assistant Professor, Computer Science and Engineering, ASRA College of Engineering and Technology, Bhawanigarh, Punjab, India*

Abstract: ***The cloud is being increasingly used to store and process the big data. The main advantage of cloud computing is cloud data storage where the data is not stored on their data servers. Cloud security is one of the most analytical aspects because of its confidential information and responsive data. Many researchers have been trying to protect big data in cloud computing environment. Here, a new security framework is provided where genetic algorithm is applied on the data when it is stored by the user. Because Genetic algorithm is a stochastic algorithm; randomness plays an important role. Genetic Algorithm considers a population of solutions. Many solutions at every iteration offer a lot of advantages. Also, for better solutions it can recombine different solutions. In the new security framework, the data is converted into binary bits. These binary bits are then divided into block of bits of size 8 bits. On every two blocks of bits genetic algorithm is applied. Only crossover and mutation Genetic Algorithm operations and pseudorandom number is used in encryption process of data. Every genetic operation generates blocks of bits which will be ciphertext. This ciphertext will be stored on cloud at different locations. An attacker cannot detect the location of ciphertext. Encrypted data parts are stored on cloud and Cloud Service Provider cannot see the encrypted data.***
Keywords: Ciphertext, Cloud Service Provider, Cloud security, Crossover, Genetic Algorithm, Mutation, Pseudorandom number

I. INTRODUCTION

Cloud computing is the virtual platform where computer system resources are available online on-demand on the internet. For example: Amazon EC2, it provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Applications can be developed and deployed faster with Amazon EC2. The example of cloud computing can be found everywhere from the small and single messaging apps to audio and video streaming services.

A. Why to Chose Cloud Computing?

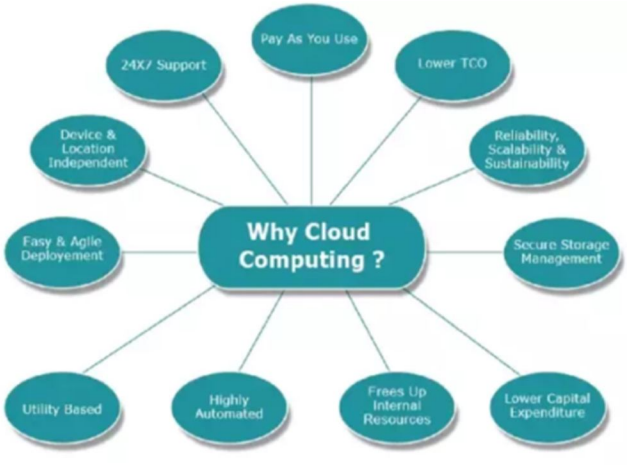


Figure 1. Advantages of cloud computing

These are the different uses and advantages of cloud computing which includes pay per use, reliability, scalability, storage management, easy and agile deployment etc. which are the reasons to use cloud computing.

©IJRASET: All Rights are Reserved

B. Cloud Application Services

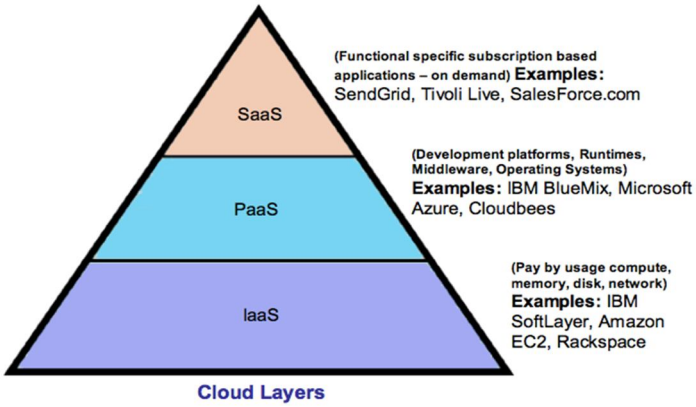


Figure 2. Cloud Layers

1) *SaaS:* Software as a Service, SaaS deliver applications to its users by utilizing the internet. There is no need of downloads or installations on the client side when using SaaS applications. Examples of SaaS are SalesForce, Google Apps, BigCommerce etc.
2) *PaaS:* Platform as a Service, PaaS provides a platform for software creation. PaaS offers high level integrated environment to build, test, and deploy custom apps.
3) *IaaS:* Infrastructure as a Service, IaaS is fully self-service for accessing and monitoring things like compute, networking, storage and other services. It allows businesses to purchase resources on-demand instead of buying the hardware or infrastructure. Example: Eucalyptus

C. Cloud Types

1) *Public Cloud:* In public cloud, computing services are available to anyone who wants to use or purchase them. The cloud provider manages all hardware, software and other supporting infrastructure. Example: Microsoft Azure
2) *Private Cloud:* In private cloud, all hardware and software are dedicated solely to the particular organization.
3) *Hybrid Cloud:* In hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options.
4) *Community Cloud:* A community cloud is shared between organizations or a specific community with a common goal.

D. What is Cloud Security?

Hello Cloud computing security is a vast service that provides services and functionalities as IT security. It includes the security of confidential data, critical information and authorized data. It protects the data from data leakage, theft, unauthorized access and breaching. Cloud security gives the ability to perform security of data in an agile manner.

II. PROPOSED WORK

The representation of proposed work is shown in Figure 3. The steps are explained here.

1) The data is taken from the user. This data is converted into ASCII values (American Standard Code for Information Interchange) using MATLAB.
2) These ASCII values will be converted into binary bits having block size of 8 bits.
3) Generate pseudorandom number using formula:

$$= (2-0)*\text{rand}+0$$

It generates random numbers between 0 and 2 because 0, 1 and 2 numbers are required to choose the crossover operation. Otherwise ‘rand’ function generates random number between [0,1]. Then apply round function on it. Save it for further use.

4) Go to user login, the user has to fill username and password. The new user has to get registered first then the new user can proceed. This is implemented in Microsoft Visual Studio.

©IJRASET: All Rights are Reserved

5) Select encryption from the process of encryption and decryption first. Genetic operations (crossover and mutation) are implemented here for security of cloud data.
6) Choose crossover operation type on the basis of output of round function of pseudorandom number. Enter the blocks of size 8 bits and generate offspring. Then apply mutation and it gives the ciphertext. Save this ciphertext. This ciphertext is used further for the process of decryption.
7) If the data is to be decrypted, select the process of decryption. It applies reverse mutation on the ciphertext. Choose crossover operation types. It is implemented in reverse during decryption process. It generates plaintext.
8) The plaintext is converted into original data in MATLAB.

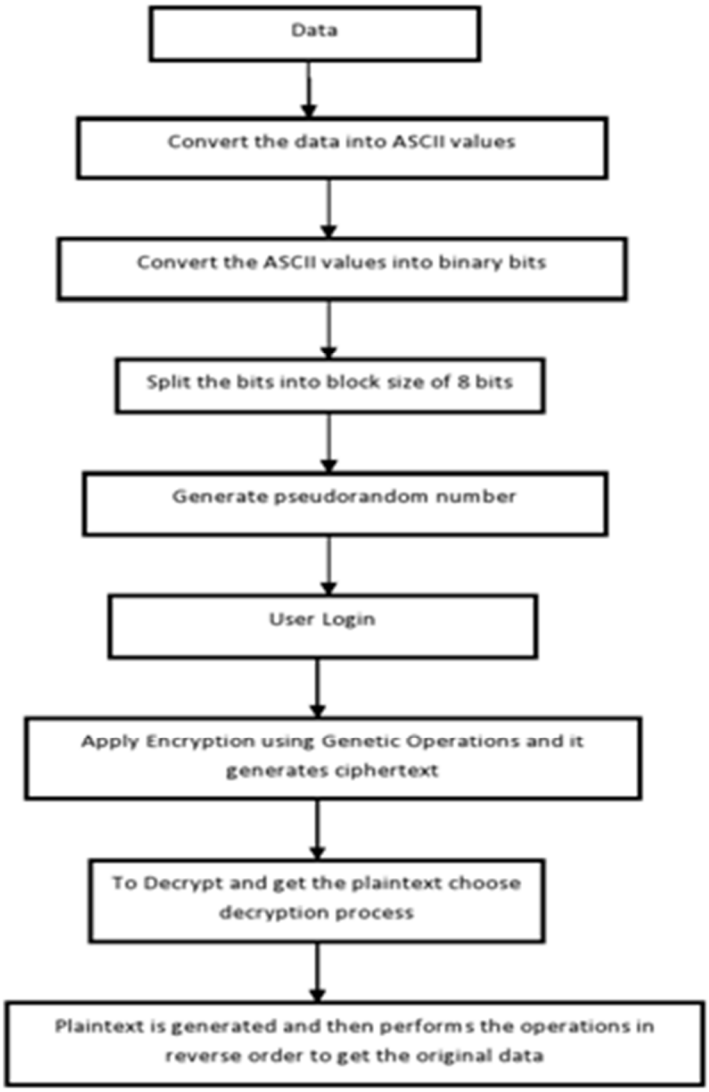


Figure 3. Representation of Proposed Work

III. ANALYSIS

In the proposed framework, the data is saved at CSP rather at DO itself. It increases security of data. The ciphertext which is generated after encryption is stored at distinct location at cloud so that an attacker cannot find the location of ciphertext. If the location is same and fixed it will be quite easy to find the location of ciphertext and hence ciphertext will be breached. GA uses less computation time as compared to key concept methods. It reduces the total computation overhead. Also, a key concept is not followed here because it will be quite difficult to maintain the security of keys and also complex to store it. Here, encryption and decryption process are done after generating random numbers.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XI, Nov 2019- Available at www.ijraset.com

IV. SIMULATION AND RESULTS

The proposed framework is implemented using MATLAB and Microsoft Visual Studio tool. Encryption is done first. In Figure 4. Data is converted into ASCII values, Figure 5. Data is converted into binary bits. Random numbers are generated as shown in Figure 6. The existing user has to login and new user has to register to proceed as shown in Figure 7. Choose crossover operation type shown in Figure 8. One point crossover is chosen here and mutated points after mutation which is ciphertext which is saved as shown in Figure 9. Then select decryption to generate plaintext as shown in Figure 10. The plaintext is converted into original data in MATLAB as shown in Figure 11.

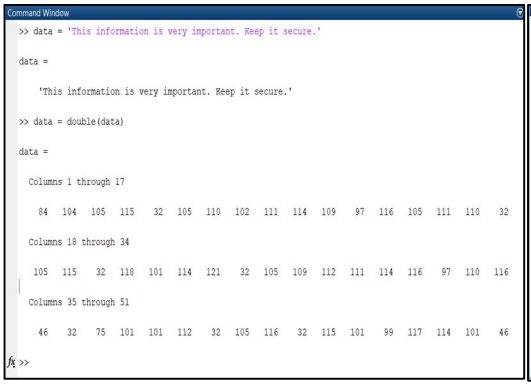


Figure 4. Converting Data into ASCII values

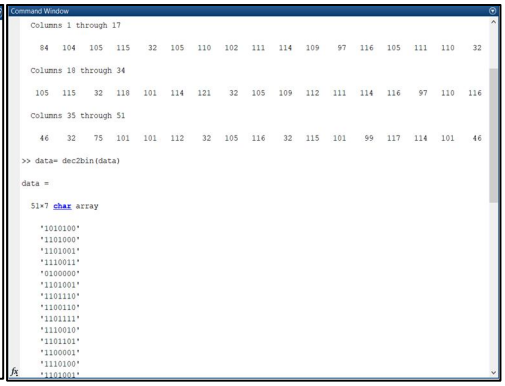


Figure 5. Converting ASCII values into binary bits



Figure. 6 Generation of random numbers

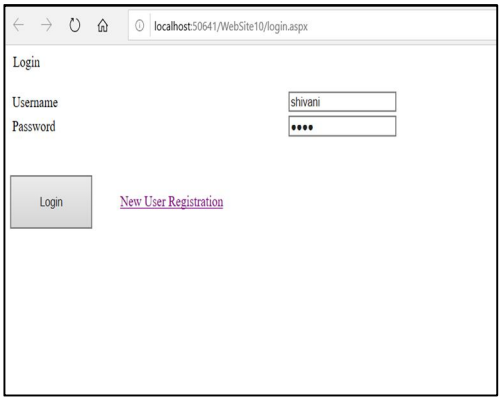


Figure 7. Login for existing user and new user can register here

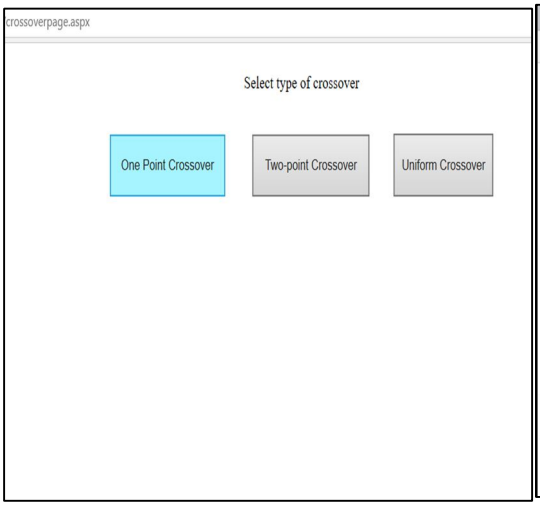


Figure 8. Choose crossover operation type

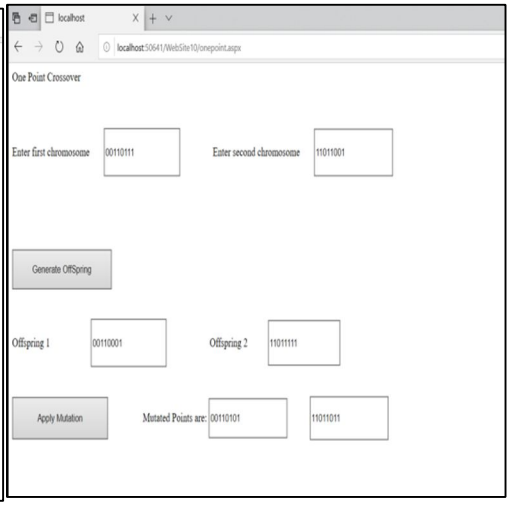


Figure 9. Ciphertext generated after mutation

©IJRASET: All Rights are Reserved

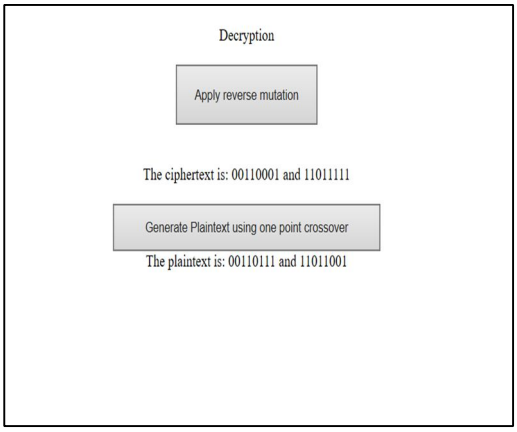


Figure 10. Plaintext generated after decryption

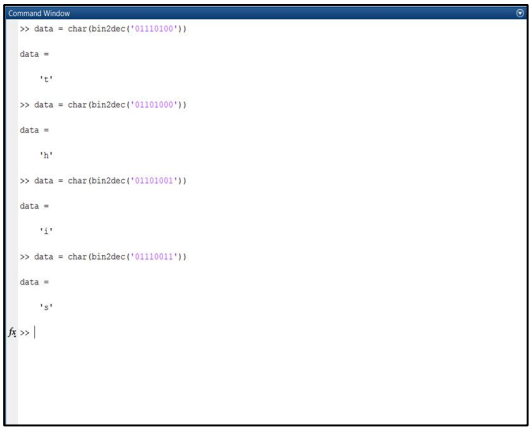


Figure 11. Plaintext is converted into original data

V. COMPARISON WITH EXISTING WORK

In this section, the existing work is compared with the proposed work. It compares the existing and proposed work in all terms.

Existing work	Proposed work
More complex as it uses pseudorandom generator function using multiplicative congruential generator to generate random number.	Fewer complex as it does not use a pseudorandom generator function but a formula to generate random number.
Space consuming because it maintains capability list.	Consumes less space as it does not maintain capability list.
More time complexity.	Less time complexity.
It takes more execution time.	Very less execution time is taken by the proposed system comparatively.

Comparison Of System By Showing Graphs

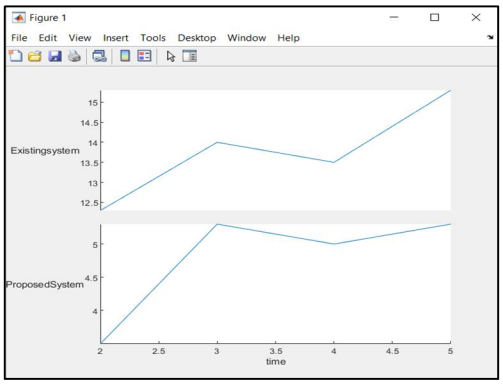


Figure 12. Graph for comparing time complexity

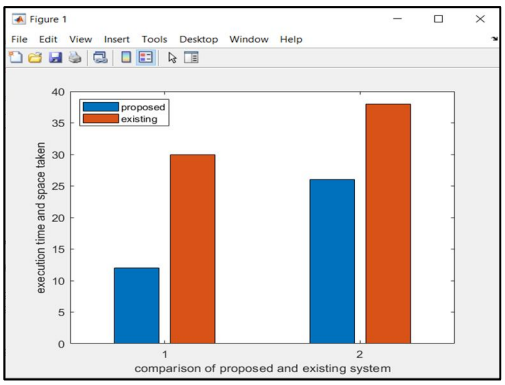


Figure 13. Bar chart comparing proposed and existing system

VI. CONCLUSION

The proposed work ensures the confidentiality and security of data. Many methods and schemes are proposed but they have some issues like vulnerability of attack, breaching of security, system performance and complexity. Cloud security is one of the crucial problem as every organization even every individual is using cloud to store data. So, it is important to make that data very secure so that only intended user can access it. Genetic algorithm provides much security and is less complex than other methodologies. Two operations are used here crossover and mutation. The proposed work do not have any key concept otherwise key is also as important as data. Therefore, no key concept is followed here. The data is so secure by applying this method therefore attacker cannot find the original data. Because ciphertext is stored at distinct locations at cloud, it would not be possible for an attacker to find it.

©IJRASET: All Rights are Reserved

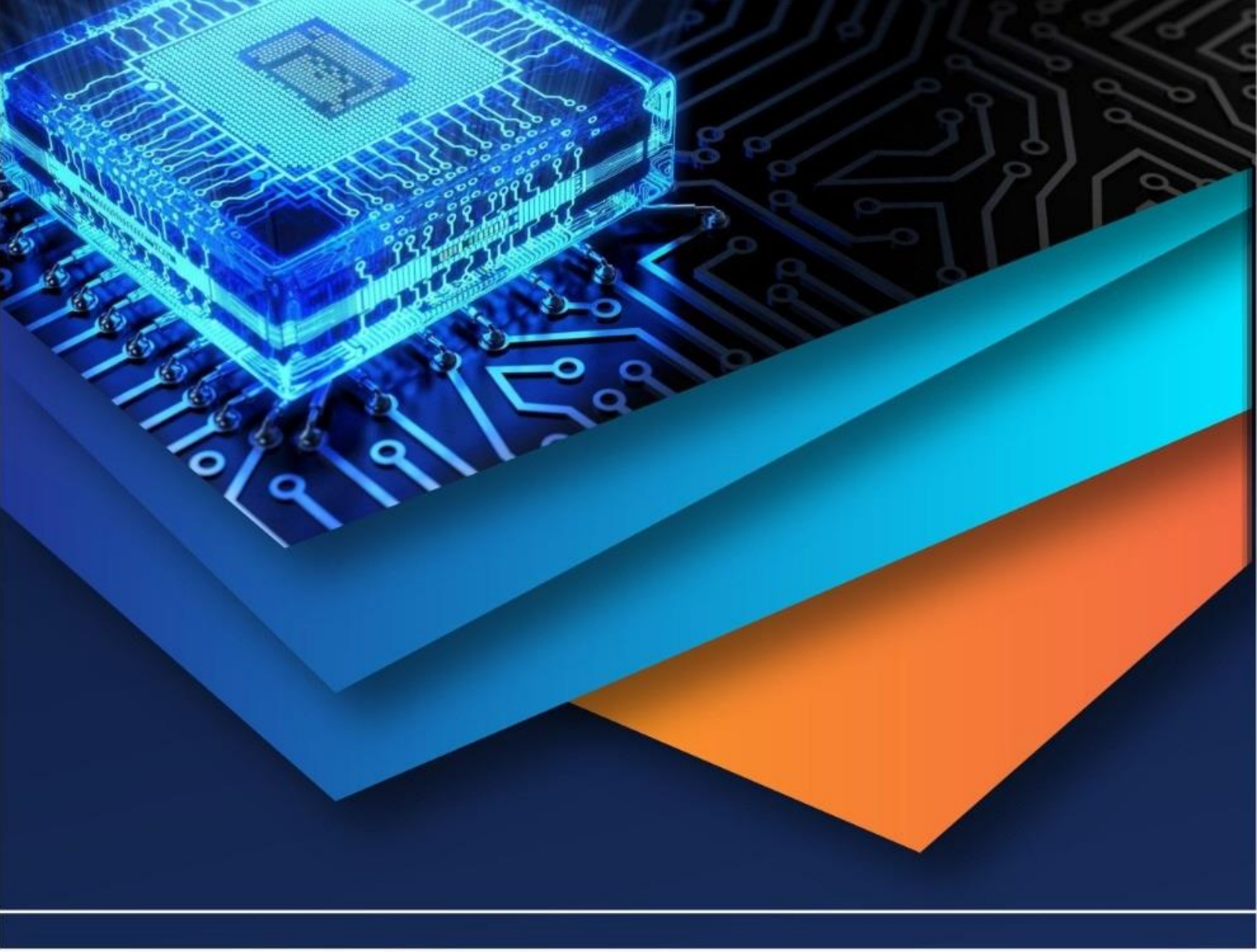
VII. FUTURE WORK AND SCOPE

Here, block size taken is of 8 bits. Block size can be smaller also. It can be of 4 bits or 2 bits etc. The number of blocks to data will also increase if block size is of smaller size correspondingly. Then genetic operations will also be more in number which will be required accordingly. Therefore, more number of random bits will be there for the corresponding data in the ciphertext. Hence, confidentiality of data increases as randomness increases. The scheme proposed here can be simulated at a platform only if these tools are integrated. Integration of tools is also one of the scopes of this proposed system. Other Genetic algorithm functions like replacement and selection can be applied in a different manner. If an unauthorized user or malicious activity is going to happen then the method can alert the system so that it is easier to detect and prevented further.

REFERENCES

[1] Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, "Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS 2016)
[2] B. Hari Krishnaa, Dr.S. Kiranb, G. Muralia,b, R. Pradeep Kumar Reddy, "Security Issues In Service Model Of Cloud Computing Environment", Procedia Computer Science 87 (2016) 246 – 251
[3] Chaimae Saadi, Habiba Chaoui, "Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb", International Conference on Computational Modeling and Security (CMS 2016)
[4] El Balmany Chawki, Asimi Ahmed, Tbatou Zakariae, "IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors", The 2nd International Workshop on Big Data and Networks Technologies (BDNT'2018)
[5] Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Ligang Cong, Jinqing Li, Huamin Yang, "Security Strategy for Virtual Machine Allocation in Cloud Computing", 2018 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2018
[6] Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Ligang Cong, Jinqing Li, Huamin Yang, "Security Strategy for Virtual Machine Allocation in Cloud Computing", Procedia Computer Science 147 (2019) 140–144
[7] Jayant D. Bokefodea, Avdhut S. Bhiseb, Prajakta A.Satarkara and Dattatray G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption", Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)
[8] Mr. Ajay Bhaisare, Prof. Ashwini Meshram, "Data Protection Outsourcing of Cloud Data to Maintain Trust between Cloud Service and Data Owner Using RC5 Algorithm", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 608-616
[9] Mr. Manish M Potey, Dr C A Dhote, Mr Deepak H Sharma, "Homomorphic Encryption for Security of Cloud Data", 7th International Conference on Communication, Computing and Virtualization 2016
[10] 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)
[11] Nandita Sengupta and Ramya Chinnasamy, "Contriving Hybrid DESCAST Algorithm for Cloud Security", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)
[12] Rizwana Shaikh, Dr. M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)
[13] Santosh Kumar Majhi, Sunil Kumar Dhal, "Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation", International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA
[14] Selvamani K, Jayanthi S, "A Review on Cloud Data Security and Its Mitigation Techniques", International Conference on Intelligent Computing, Communication and Convergence (ICCC- 2015)
[15] ShaluMall, Sushil Kumar Saroj, "A New Security Framework for Cloud Data", 8th International Conference on Advances in Computing and Communication (ICACC-2018)
[16] Vishruti Kakkada, Hitarth Shaha,Reema Patela, Nishant Doshi, "A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing", Procedia Computer Science 155 (2019) 680–685

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)