DEVELOPING AN INTEGRATED SYSTEM BASED ON GENETIC ALGORITHM TO ENHANCE SECURITY SAFEGUARD IN CLOUD COMPUTING ENVIRONMENT

Namrata Deswal

GD Goenka World Institute Lancaster University, Gurugram, Haryana

ABSTRACT:

The cloud is progressively used to store and deal with vast amounts of information. The main benefit of distributed computing is cloud information capacity, where the data isn't put away on their information servers. Cloud security is perhaps the most insightful viewpoint due to its classified data and responsive information. Numerous analysts have been attempting to safeguard enormous information in a distributed computing environment. Here, another security system is given where the genetic calculation is applied to the data when the client stores it. Since a Genetic calculation is a stochastic calculation, arbitrariness assumes a significant part. The genetic Algorithm thinks about a populace of arrangements. Numerous arrangements at each emphasis offer a ton of benefits.

Additionally, for better arrangements, it can recombine various accounts. The information is changed over into twofold pieces in the new security system. These twofold pieces are then separated into blocks of pieces of size 8 bits. On each two-block of parts, a genetic calculation is applied. Just hybrid and transformation Genetic Algorithm tasks and the pseudorandom number are utilized in the encryption cycle of information. Each inborn capacity creates blocks of pieces that will be ciphertext. This ciphertext will be stored in the cloud in various areas. An aggressor can't distinguish the size of ciphertext. Encrypted information parts are put away in the endless cloud Service suppliers can't see the encoded information.

I. INTRODUCTION

Distributed computing is the virtual stage where PC framework assets are accessible online on request on the web. For instance, Amazon EC2 gives adaptable figuring limits in the Amazon Web Services (AWS) cloud. Applications can be created and sent quicker with Amazon EC2. The case of distributed computing can be found all over the place, from the minor and single informing applications to sound and video web-based features.

A. Why Choose Cloud Computing?

The various purposes and benefits of distributed computing incorporate compensation peruse, dependability, versatility, the capacity of the board, reasonable and coordinated arrangement, and so on. These are the purposes behind utilizing distributed computing.

1) SaaS: Software as a Service, SaaS conveys applications to its clients using the web. There is no requirement for downloads or establishments on the client-side while utilizing SaaS applications. Instances of SaaS are SalesForce, Google Apps, BigCommerce, and so forth.

2) PaaS: Platform as a Service, PaaS gives a stage to programming creation. PaaS offers an undeniable level of incorporated climate to assemble, test, and convey custom applications.

3) IaaS: Infrastructure as a Service, IaaS is self-administration for getting to and checking things like registering systems administration, stockpiling, and different administrations. It permits organizations to buy assets on request rather than the equipment or foundation.

B. Model: Eucalyptus

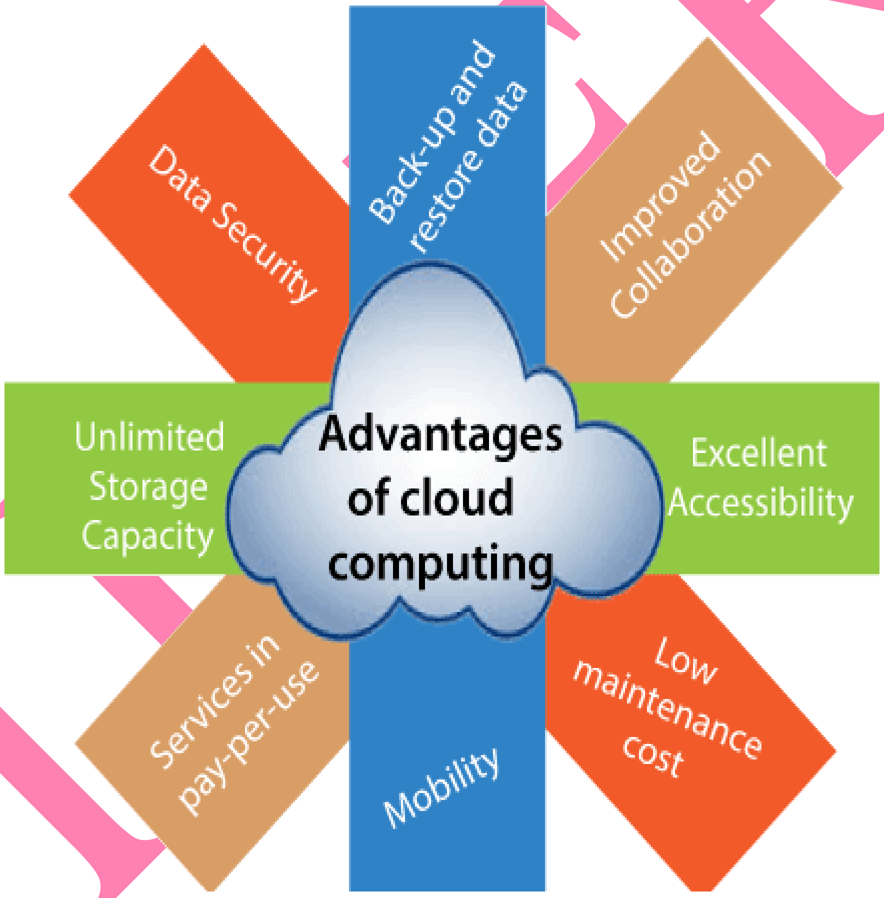


Figure 1: Advantage of Cloud Computing

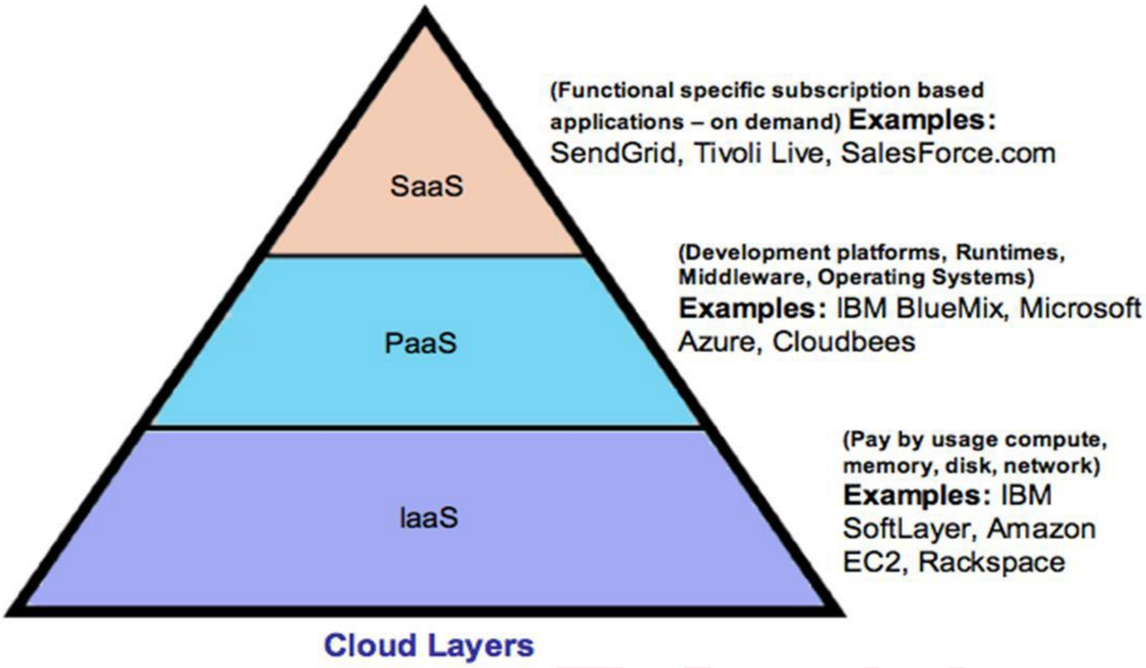

SaaS
PaaS
IaaS
(Functional specific subscription based applications – on demand) Examples: SendGrid, Tivoli Live, SalesForce.com
(Development platforms, Runtimes, Middleware, Operating Systems) Examples: IBM BlueMix, Microsoft Azure, Cloudbees
(Pay by usage compute, memory, disk, network) Examples: IBM SoftLayer, Amazon EC2, Rackspace
Cloud Layers

Figure 2: Layer of Cloud

C. Cloud Types

1) Public Cloud: In the public Cloud, figuring administrations are accessible to any individual who needs to utilize or buy them. The cloud supplier deals with all equipment, programming, and another supporting framework. Model: Microsoft Azure

2) Private Cloud: All equipment and programming are devoted exclusively to the specific association in a private cloud.

3) Hybrid Cloud: In a half-breed cloud, information and applications can move among private and public mists for more noteworthy adaptability and excellent transmitting options.

4) Community Cloud: A people group cloud is divided among associations or a particular local area with a shared objective.

D. What is Cloud Security?

Hi, Cloud figuring security is tremendous assistance that offers types of aid and functionalities as IT security. It incorporates protecting private information, primary data, and approved reports. It safeguards the data from information spillage, robbery, unapproved access, and penetrating. Cloud security provides the capacity to perform information security elegantly.

II. PROPOSED WORK

The portrayal of the proposed work is displayed in Figure 3. The means are made sense here.

1) The information is taken from the client. MATLAB changes over this information into ASCII values (American Standard Code for Information Interchange).

2) will change these ASCII values into double pieces with a block size of 8 pieces.

3) Generate pseudorandom number utilizing the recipe:

= (2-0)*rand+0

It creates arbitrary numbers somewhere in the range of 0 and 2 since 0, 1, and 2 are expected to pick the hybrid activity. In any case, the 'rand' work produces an arbitrary number [0,1]. Then apply the around cycle to it. Save it for additional utilization.

4) Go to client login. The client needs to fill username and secret phrase. The new client needs to get enlisted first. Then, at that point, the new client can continue. This is executed in Microsoft Visual Studio.

5) Select encryption from the course of encryption and decoding first. Hereditary tasks (hybrid and change) are executed to get cloud information.

6) Choose a hybrid activity type in light of a round capacity of pseudorandom number. Enter the blocks of size eight pieces and create posterity. Then, at that point, apply the change, giving the ciphertext. Save this ciphertext. This ciphertext is utilized further for the course of unscrambling.

7) If the information is decoded, select the course of unscrambling. It applies to switch transformation to the ciphertext. Pick hybrid activity types. It is executed backward during the decoding system. It produces plaintext.

8) The plaintext is changed over into unique information in MATLAB.

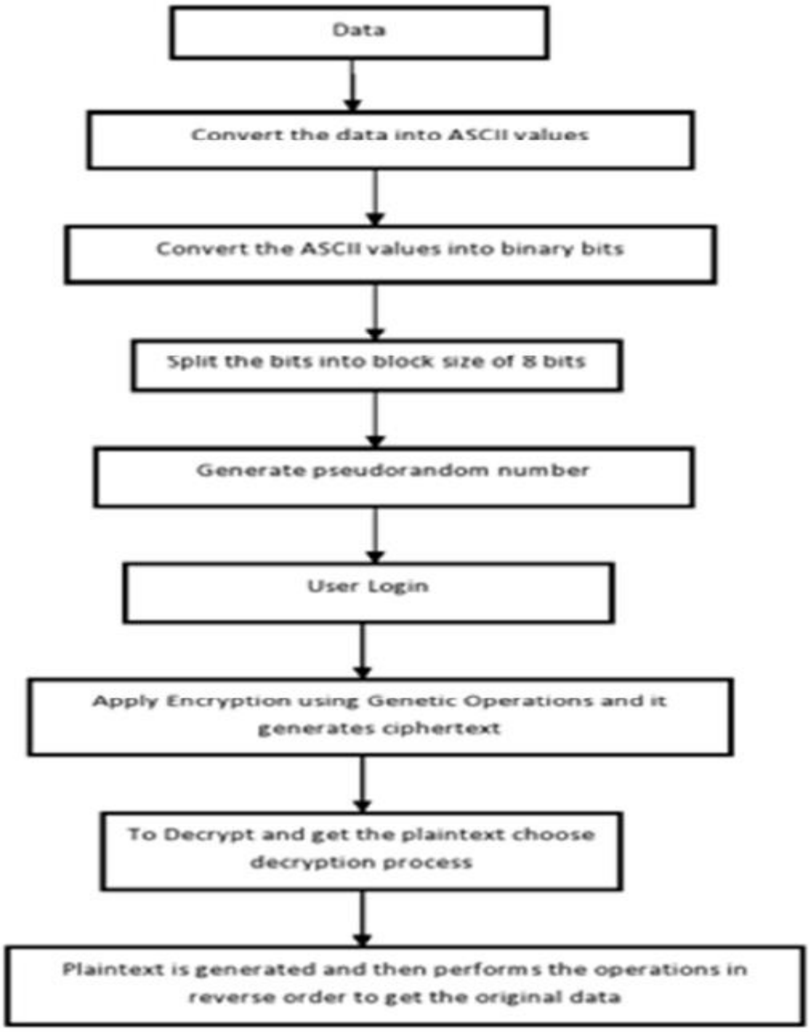

Data
Convert the data into ASCII values
Convert the ASCII values into binary bits
Split the bits into block size of 8 bits
Generate pseudorandom number
User Login
Apply Encryption using Genetic Operations and it generates ciphertext
To Decrypt and get the plaintext choose decryption process
Plaintext is generated and then performs the operations in reverse order to get the original data

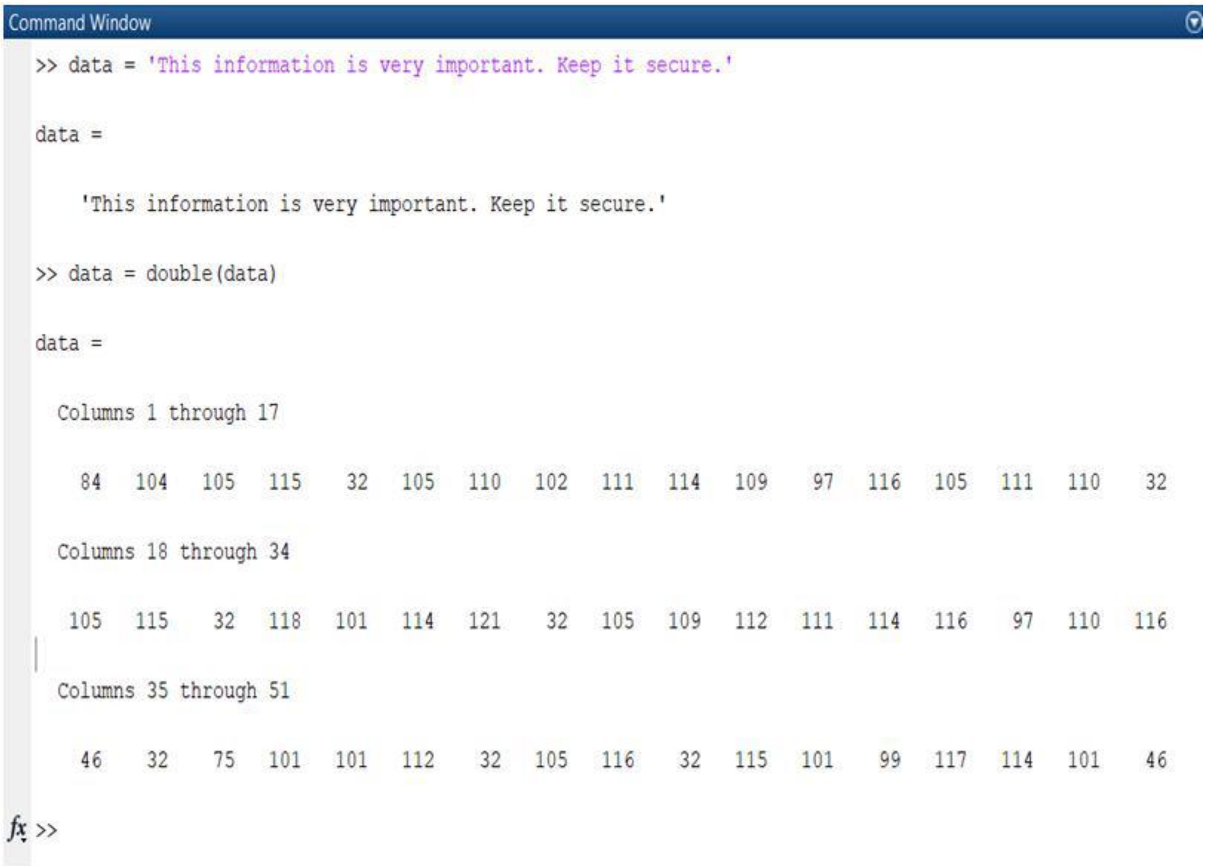
Figure 3: Proposed Work Representation

III. EXAMINATION

The information is saved at CSP in the proposed structure rather than at DO itself. It builds the security of data. The ciphertext, which is produced after encryption, is put away in a particular area in the Cloud with the goal that an assailant can't track down the spot of the ciphertext. Assuming that the site is something very similar and fixed, it will be pretty simple to track down the area of ciphertext, and henceforth ciphertext will be penetrated. GA utilizes less calculation time when contrasted with required idea techniques. It decreases the all-out calculation upward. Additionally, a key idea isn't followed here since it will be challenging to keep up with the security of keys and the complex to store them. Here, the encryption and decoding process is done in the wake of creating arbitrary numbers.

IV. REENACTMENT AND RESULTS

The proposed system is carried out utilizing MATLAB and Microsoft Visual Studio devices. Encryption is done first in Figure 4. Information is changed over into ASCII values.



```
>> data = 'This information is very important. Keep it secure.'

data =

    'This information is very important. Keep it secure.'

>> data = double(data)

data =

  Columns 1 through 17

    84   104   105   115    32   105   110   102   111   114   109    97   116   105   111   110    32

  Columns 18 through 34

   105   115    32   118   101   114   121    32   105   109   112   111   114   116    97   110   116

  Columns 35 through 51

    46    32    75   101   101   112    32   105   116    32   115   101    99   117   114   101    46

fx >>
```

Figure 4: Ascii Values

IV. CORRELATION WITH EXISTING WORK

In this segment, the present work is contrasted and the proposed work. It looks at the current and proposed work in all terms.

V. CONCLUSION

The proposed work guarantees the classification and security of information. Numerous strategies and plans are offered. However, they have a few issues like assault weakness, break of safety, framework execution, and intricacy. Cloud security is one of the critical issues as each association, even every person, utilizes the Cloud to store information. Thus, making that information exceptionally secure is vital, so just the planned client can get to it. The hereditary calculation gives a lot of safety and is less intricate than different philosophies. Two activities are utilized here hybrid and change. The proposed work has no significant idea; in any case, the key is just about as substantial as the information. In this manner, no key though is followed here. The data is so secure by applying this technique that an aggressor can't track down the first information. Since ciphertext is put away in particular areas in the Cloud, an aggressor wouldn't be able to track down it.

VI. FUTURE WORK AND SCOPE

Here, the block size taken is eight pieces. Block size can be more modest too. It very well may be of 4 bits or two pieces. The number of blocks to information will likewise increment, assuming that the block size is of more modest size. Then hereditary tasks will be more in number, which will be required appropriately. Hence, more irregular pieces will show up for the ciphertext-related information. Subsequently, the classification of information increments as haphazardness increments. Can reenact the proposed plan at a stage provided that these devices are incorporated. The mix of gadgets is likewise one of the extents of this proposed framework. Can apply other Genetic calculation capacities like substitution and determination unexpectedly. If an unapproved client or malevolent action occurs, the strategy can caution the framework, making it more straightforward to distinguish and forestall 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