CLOUD DATA SECURITY FRAMEWORK USING GENETIC ALGORITHM

P. Murugeswari
Assitant Professor
Department of Information Technology,
GTN Arts College, Dindigul, Tamilnadu, India.

Abstract : In many organizations and organizations, the use of cloud has increased quickly. Cloud data storage is one of the main advantages of cloud computing, where the data owners. On this end, cloud safety is one of the most given to getting details aspects because of, in relation to the to be kept secret information and sensitive data . This paper presents a new safety framework which provides more data safety and secretly. In the new safety framework, a data is spilt in the blocks of bits. Genetic algorithm is applied on every block of bits. Last out-put of every genetic algorithm operation is a cipher text which is also blocks of bits. Each cipher text is stored on cloud at separate placing and placing of the cipher text is not fixed. So, it is hard for an attacker to detect where cipher text is in addition, genetic algorithm has no key idea of a quality common to a group because of, in relation to which safety of data increases. The new safety framework puts to use genetic algorithm on smaller block size which increases the safety. The framework also uses the power to do list for safe and fine grain way in of data.

IndexTerms - Genetic Algorithm; Crossover; Mutation; Data Splitting; Cloud Storage; Outsourced Data;

I. INTRODUCTION

Cloud computing is very having general approval and quick getting greater, stronger, more complete technology in deeply rooted way of acting as well as organizations because it gives computing services and place for storing of data at very good-looking price The advantages of using cloud computing technology including simple, not hard scalability, price saving, and high able to use. Now days, the cloud is very essential and key aspect among every technology which includes the identity business managers virtualization safety, application true, good nature, network safety and data cares. In the above order of events, data care is very essential in cloud computing. In cloud computing, there are three types of Service model namely- IaaS(Infrastructure as a Service)- In IaaS users get resources like cpu time, network bandwidth, processing power and place for storing. Once the person getting goods from stores gets the base structure he may control the OS, application, data host-based safety, services and so on. PaaS(Platform as a Service)- In PaaS users are on condition that the hardware roads and systems, OS and network to make a hosting environment. From the hosting environment, user can activate services and put in position of authority his applications. SaaS (software as a Service)- In SaaS, users are on condition that the way in to an application. They have no limit over the network, hardware, OS or safety. The Cloud computing has five major points: network way in, on request self-helping, resource pooling, quick elasticity, placing Independent. These all characteristics made the cloud significant. Organizations and industries are increasing their income and profited by making use of these cloud computing characteristics [2]. This is the reason; industries are moving their business to cloud. But safety of data 3 is a major 23 limit in cloud computing. In present time, cloud safety is one of the biggest critical issues in the environment of cloud computing because of, in relation to the sensitive data of data owner (DO). So, cloud Service giver (CSP) must take into account safety and right not to be public issues in high right of coming first. The data of DO is got ready and kept safe on outside servers. So, true, good nature, secretly as well as data way in control become more important and essential. Since, the outside servers are managed through money-related Service givers, DO cannot Trust on them as they can use its data for their profit and can make of no use the business of DO. Even, DO cannot Trust on clients or users connected to it, as they can be full of ill feelings and bad. Secretly of sensitive data can be breached over Service givers. There are some frequent carefully worked designs on condition that to protect data although they are in pain or troubled from several Issues. Here, we present a new safety framework to safe the data of DO which is stored on cloud [2][8][9][10].

II. RELATED WORK

Data way in control and secretly are necessary safety measures for outsourced data. Once, when we indicate further on safety of data, we not be able to have in mind about systems doing a play (CSP, do, users). For example, sometimes we use more keys to safe the data. To store, maintain, get and make distribution the keys are Total computational over-head. Generally, keys are either stored by DO or by Third-Party over-seer (TPA). But there are many alternatives to easily way in data in cloud by using the keys stored in TPA. And we should also make certain the level of secretly and way in control. Remarkably, there is a carefully worked design needed that not only provides data safety but also support the work of the system. There are many carefully worked designs are given below to safe the data. Design offered in [3] using third Party over-seer, number without thought of amount function and RSA. In this design, the third-party over-seer (TPA) is taken into account in active and acts all the computations and verifications. It is experienced that we cannot fully Trust on TPAs, that it can use the data of DO for own get money for profit. Another getting well field in offered design [3] is breaking the RSA much simple than factoring [4]. Design offered in [5] is safe, good, and ready to make money for way in control and secretly of data. In this carefully worked design, the Author encrypts data through secret- keys and these keys are only took in to DO and corresponding data users. The encrypted

files are stored at CSP. During the communication between CSP and the user, data are further encrypted through one-time private meetings key which is shared among CSP and the user through the made different diffie-hellman protocol. This design provides full data safety but there is a key corresponding to every file and user but in some applications, files and users may be complex in numbers. So, there may have a complex number of keys. Design offered in [6] using Shamir having the same algorithm with CRT (chinese rest theorem) which gives to the key and shares the key among one taking part support givers. Here, numbers of keys are reduced but the design has no Arrangement of managing data. design offered in [7] using the cryptographic data making into mechanism with aes algorithm which divide the users encrypted file into parts and stored on public cloud but there is no given credit for related to key. The offered design some-how matches with designs [7][11][12] but is much safer.

III. REPRESENTATIONS

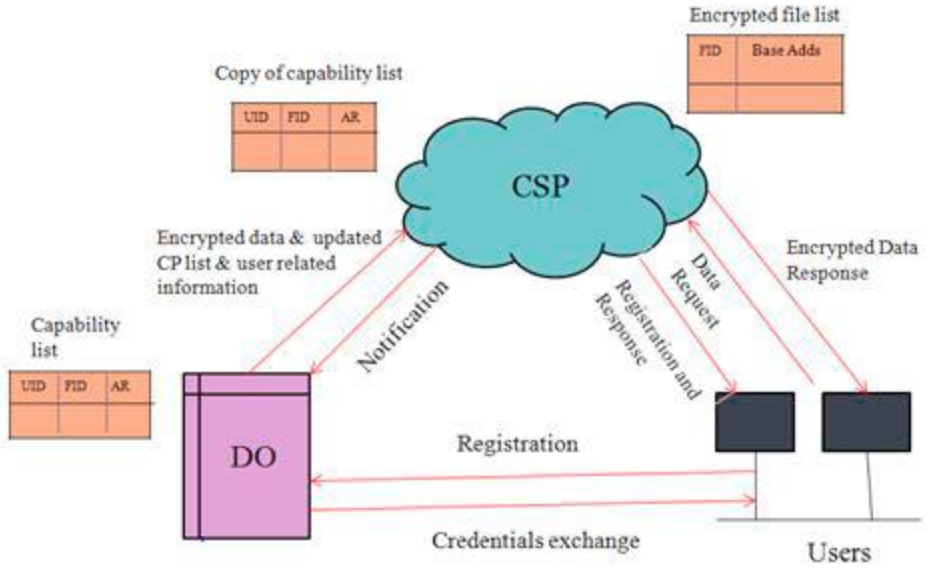


Fig 1. Communication Method

We take to be true that the offered design is chiefly of three things DO, CSP and many users connected with DO. Firstly, every user is said to be true at DO. For the period of process of getting official support material, users send their experience, knowledge/ needed information to DO. We take as probable that the users credential is sent to DO safely during the number on a list. And after with a good outcome the number on a list, DO send needed information pseudorandom number and information related crossover and mutation operations) to the user safely in move. We also take to be true that DO have some processing power to do and space to store some data. DO store its data to CSP. After with a good outcome checking to make certain of the user to CSP, the user can get back data from CSP in some secret way. We take to be true that CSP knows and has mechanisms to give position of and store the data. CSP are greatly-sized organizations they have such type of mechanisms. Fig.1 shows the communication among DO, CSP and users.

GA	Genetic Algorithm
FID	File Identity
DO	Data Owner
AR	Access Right
CSP	Cloud Service Provider
CP List	Capability List
AES	Advanced Encryption Standards
TPA	Third Party Auditor
RSA	Rivest Shamir Adleman
PRN	Pseudo Random Number
E	Encryption
PUCSP	Public Key
CSP D	Decryption
PRCSP	Private Key of CSP
UID	User Identity
PRDO	Private key of DO

Table1:Nomenclature

IV PROPOSED METHOD

The new security framework

In the offered careful way, we give the new safety framework for data that is stored on the cloud. In this safety framework, a data is not changed into ascii values. Then these ascii values are got changed into binary bits then divided into blocks of bits of some size. Block size may be 8 bits, 4 bits, 2 bits and so on. Here, genetic algorithm (Ga) operations (crossover and mutation) are used for encryption and process of changing knowledge back into starting form process. Ga operations (crossover and mutation) are applied on each pair of blocks. The last out-put of each Ga operations is a cipher text which also pair of blocks of bits. Each cipher text is stored on cloud at separate placing and, placing of cipher text is not fixed (for example, output1 stored in the cloud has placing l1 at times t1 may have placing l2 at times t2 by some mechanisms. Since, encrypted data parts are stored on cloud, CSP is not able to see the data. Before sending to CSP, these encrypted data parts are further encrypted with private key of DO for DO checking to make certain and, then encrypt the encrypted data with public key of CSP again so that attacker is not able to see the data and CPList. The complete work Procedure of the new design is made clear in Fig.2. Here, there are some terms or functions which are used in encryption or process of changing knowledge back into starting form process of data. And, also make, be moving in here how Ga works **Genetic Algorithm**

Genetic algorithm (Ga) [11] is a group of three processes replacement, selection and genetic operation (crossover, mutation). In this paper, only genetic operations (crossover, mutation) and pseudorandom number are used in encryption process of data which are described as comes after:

Pseudorandom Number-It is a random number which is used in decision to which crossover function should select for crossover operation.

Pseudorandom Number Generator-There are a variety of techniques by which a random number is produced, however the generally used technique is multiplicative congruential generator. coming here-after is the function which is used to generate false random number-

$$x_{i+1} = x_i.c \text{ (modulo m)}$$

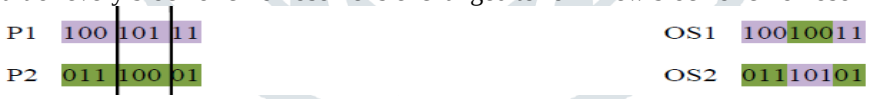
where xi+1 is the subsequent Pseudo Random Number(PRN) of xi, c and m are +ve integer number, c is frequently multiply by xi and the outcome is xi.a and it is divided by m. As far as the remainder comes less than m.x0 is the first number by which we start calculating the PRN. In pseudo random number 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 chromosomes or blocks of data [11].

Crossover

It is the process in which two blocks or chromosomes are taken to generate a new offsprings or children. There are mainly three crossover operations which are used on binary coded GA.

- One-point crossover-In one-point crossover two blocks (P1 and P2) are given, randomly two chromosomes are chosen and broken the blocks into half then tails of two chromosomes is exchanged to obtain new off springs (OS1 and OS2).

- Two-point or Multi-point crossover-It is related to one-point crossover excepting two cut points are created instead of one, then one part of every block or chromosome is exchanged to form new block or chromosome.



- Uniform crossover-In uniformcrossover, the bits are copied randomly from the 1st and 2nd point. In this operator we do not divide the blocks into pieces and the random mask is generated, and the mask determine which bit is copied from 1st point and which from 2nd point.

Random mask generated randomly i.e. 11010110

Mutation

Basically, the mutation is based on random changes; it changes 0 to 1 and vice versa. It is performed on two selected chromosomes or blocks.

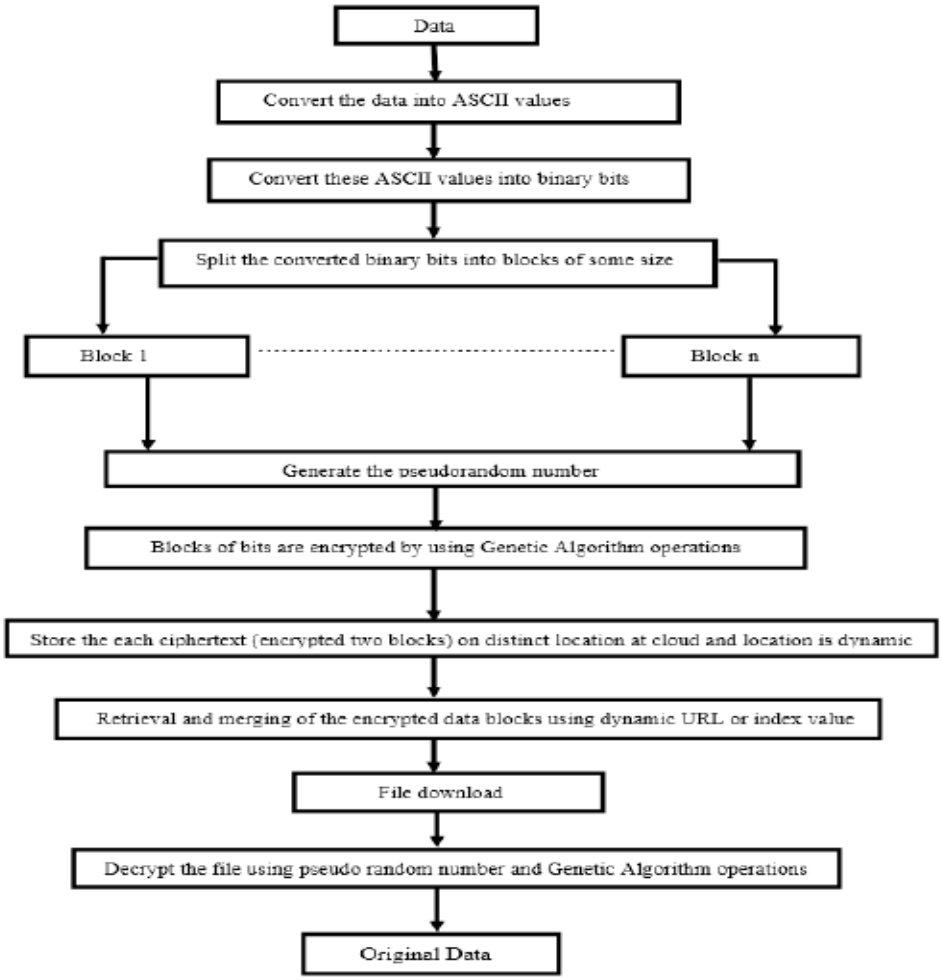


Fig 2. Security framework of proposed scheme

Algorithm 1.1: User Registration Process

Step-1: The User sends registration request to DO with his details

Send (User details)

Step-2: After successful registration, DO sends required information (random number, UID, FID, AR and few information about GA) to the User

Step-3: DO updates the capability list at its end

CPList = Add (CPList, (UID, FID, AR))

Step-4: DO encrypts the data and CP List and send it to the CSP

Send ($E_{PU_{CSP}}(E_{PR_{DO}}(E_{GA}(Data) \| CP\ List))$)

Step-5: CSP decrypts the received information from DO using his private key

$E_{GA}(Data) \| CP\ List = D_{PR_{CSP}}(D_{PU_{DO}}(E_{GA}(Data) \| CP\ List))$

Step-6: CSP updates the capability list at its end with entries sent by the DO

CPList = Add (CPList, (UID, FID, AR))

and store the encrypted data parts (each ciphertext) at distinct location

on the cloud and the location where each ciphertext is stored, is dynamic

Step-7: Now, the User can precisely connect to CSP to fetch his data.

In the proposed scheme, we used four algorithms. Algorithm 1.1 describes the registration process [1]. Algorithm 1.2 describes the splitting process of data [12]. Algorithm 1.3 describes the encryption process of data using GA and Algorithm 1.4 describes the decryption process of data using GA [11].

Algorithm 1.2: Split Algorithm

Step-1: Data is converted into ASCII values first.

Step-2: ASCII values of data then converted into binary bits

Step-3: DO splits the binary bits into n blocks of some size

Step-4: Make the new folder and save these blocks of bits

Step-5: Generate pseudo random number

Step-6: Select two stored blocks of bits for encryption

Step-7: Apply GA on selected two blocks of bits for encryption

Step-8: Then store the encrypted data parts(ciphertext) on distinct location of cloud

Algorithm 1.3: Encryption Process

Step 1: Choose two blocks of bits from storage

i.e. s_1=10001110 s_2=10001011

Step 2: Generate pseudorandom number using the pseudorandom function for selected two blocks of bits. Apply modulo operation (mod of 3) on the generated pseudorandom number

Step 3: Crossover function is chosen according to the output of the mod function

If output = 0 then Single point crossover is applied

If output = 1 then two-point crossover is applied and,

If output = 2 then uniform crossovers is applied

Example: 23%3=2 (Uniform crossover), 63%3=0 (Single point crossover)

Step 6: Apply the chosen crossover function on selected two blocks of bits

Step 7: Apply mutation function on the output of crossover function i.e. also two blocks of bits

Step 8: Output of mutation function is ciphertext (two blocks of bits) which is stored on cloud at distinct location and the location where ciphertext is stored, is not fixed

GA operations with smaller block size

Here, we send in name for encryption and process of changing knowledge back into starting form on blocks where each block size is 8 bits. We can also send in name for encryption and process of changing knowledge back into starting form process on smaller block size (4 bits or 2 bits and so on.). If, we work with smaller block size then number of blocks corresponding to a data increase. Number of Ga operations increase as number of blocks increase. So, to encrypt a data, more number of Ga operations will have need of. So, cipher texts corresponding to a data have more number of random bits. For this reason, secretly of data increases as randomness increases.

Data Retrieval from cloud

When a user wants to way in a data, he should first send data request to CSP. The user sends data request with information (UID, FID, AR) to CSP. CSP matches sent (UID,FID, AR) with stored (UID,FID,AR) for a data. If matches, checking to make certain is with a good outcome. CSP then gets back the data parts from placing 1, placing 2, Placing N using dynamic url Then complete work parts of a data are merged and stored in the users server as store, from where data is downloaded and changed back into starting form.

Capability list

The new design uses the power to do list (CP List) for safe and fine grain way in of cloud data. Basically, Cp list has uid fid and AR Entries corresponding to each data. It is basically row-based decomposition of way in matrix. In CP list, operations and took in data for a user are described. DO have a right to execute the activity and CSP read this activity for the objective of safely way in the data.

Algorithm 1.4: Decryption Process

Step 1: One ciphertext is selected from the storage of ciphertexts of a data which are sent by CSP to the user after authentication

Step 2: Apply mutation function on the selected ciphertext in reverse order

Step 3: Read the random number that is sent to the user corresponding to that ciphertext and perform modulo function (mod 3) on the random number

Example: 63%3=0 (Single point crossover), 23%3=2 (Uniform crossover)

Step 4: According to the output of mod function, perform the crossover function on the output of mutation function in reverse order

Step 5: Output of crossover function is a plaintext (two blocks of bits)

Step 6: The process from Step 1 to Step 4 are repeated until all the ciphertexts corresponding to a data are not converted into plaintexts

Step 7: Convert the binary bits of data into ASCII values

Step 8: Convert the ASCII values into texts that is the original data

V PERFORMANCE AND SECURITY ANALYSIS

ANALYSIS OF SECURITY

Here, we discuss about the strength of the new scheme and, security of outsourced data [8][9][10].

Data Confidentiality- In the new design, DO encrypts its data itself with Ga. since, Ga information are experienced only to DO and corresponding data user, only corresponding data user can see the data. CSP and attackers is not able to see the data. DO again encrypt that encrypted data with public key of CSP using public key cryptography so that attacker is not able to see the encrypted data as well as CP List. Here, CSP can see only the CP List. Here, data secretly is increased because of, in relation to double encryption. In related works, there are so many designs suggested to safe the data, but all have used the cryptographic designs which have keys for all types' encryptions. In this design, data is encrypted with Ga which has no idea of key which increases data secretly more because key is as important as data. If, key is put at risk data may be changed back into starting form. in addition, the new design does not encrypt complete work data or file at once. Here, data is first divided into number of blocks of bits. blocks of bits are selected for encryption process at a time. Each pair of blocks of bits is encrypted with Ga. And, each pair of blocks may have different Ga operations. So, to decrypt a complete work data, there may need to act many and different Ga operations. So, it is hard for an attacker to decrypt a complete work file or data. The out-put of each Ga is cipher text (blocks of bits). Each cipher text is stored on the cloud at separate placing, which increases secretly of data. in addition, the placing of cipher text is dynamic , so attacker is not able to uncertain ideas in mind where cipher text is stored. For this reason, safety of the data increases greatly. If a data is divided into smaller blocks, then number of blocks increases corresponding to a data. For this reason, more number of separate Ga operations is needed to encrypt a complete work data. So, got cipher texts of a complete work data have more random bits. For this reason, secretly of a data increases as randomness increases. In addition, most of the

currently in existences designs have the single placing for place for storing one cloud datacenter. The major unhelped side of using single placing for place for storing on a cloud data center is that, if attacker attacks on cloud the complete work data will be made way in readily. So, to make good this safety Issue, the new design stores the encrypted data parts on different places on CSP.Since, data are encrypted by use of pseudorandom number which is only experienced to DO and separate use, DO and separate user can decrypt the data.

Entity Authentication- In this design, user is made certain at DO when he forwards his own details to DO during the the number on a list. DO and CSP have made certain each other at CSP when DO sends encrypted data and CP List to the CSP because DO encrypt the data using his private key. The user is made certain at CSP when he requests for data by sending his UID FID AR and CSP make a comparison of it with related stored UID FID AR of a data.

- **Data Access Control-** The new design uses the CP List for safe and fine grain way in of cloud data. In CP list, operations and took in data for a user are given a detailed account of. Some designs have used the way in Control List (ACL). But CP List is superior to ACL because ACL gives a detailed account of users and their given authority operations for each data and it is almost inefficient that users have need of same data and have same operations on it. ACL exists without the scalability and fine grain way in of data.

Analysis of Performance

The new design, DO has moved its maximum computation and load to CSP and only did few important things by it-self. The new design has reduced the addition of computation time by using Ga because there is no key idea of a quality common to a group used in Ga. As, we have knowledge of that to store, maintain, get and make distribution the keys safely is hard, hard and Total computational over-head.

VI CONCLUSION

The new design makes certain the safety of data which are stored on CSP. Many designs are presented for safety of data , but they have some issues such as feebleness of attack, feeble amount of fine grain control of way in and system operation. because of, in relation to complex number of keys, secretly of data and doing a play of system drops. But, the new design uses Ga operations (crossover and mutation) which has no key idea of a quality common to a group. In the design, Ga is applied in nothing like it way and data are stored at separate places on the cloud in get way. Ga makes certain the data secretly. The design has used the power to do list to make certain the fine grain control way in.

References

[1]Saroj, Sanjeev Kumar Chauhan, Aravendra Kumar Sharma and Sundaram Vats. (2015) "Threshold Cryptography Based in Cloud Computing." IEEE International Conference on Computational Intelligence & Communication Technology:

[2] Jeong-Min Do, You-Jin Song and Namje Park. (2011) "Attribute Based Proxy Re-encryption for Data Confidentiality in Cloud Computing Environments."First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering,:248-251 .

[3] Preeti Garg and Vineet Sharma. (2014) "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function." IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT):334-339.

[4] Don Boneh,and Ramarathnam Venkatesan. (1998) "Breaking RSA May Be Easier Than Factoring."Lecture Notes in Computer Science: 59-71.

[5] Sunil Sanka, Chittaranjan Hota and Muttukrishnan Rajarajan. (2010)"Secure data access in cloud computing." IEEE 4th International Conference on Internet Multimedia Services Architecture and Application:1-6.

[6] Doyel Pal, PraveenkumarKhethavath, Johnson P.Thomas, and Tingting Chen. (2015) "Multilevel Threshold Secret Sharing in Distributed Cloud."Springer International Symposium on Security in Computing and Communication Cham:13-23.

[7] Balasaraswathi V. R. and Manikandan S. (2014) "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach."IEEE International Conference on Advanced Communications, Control and Computing Technologies:1190-1194.

[8] W.Stallings. "Cryptography and network security."LPE Fourth Edition.

[9] Mrinal Kanti Sarkar and Sanjay Kumar. (2016) "A framework to ensure data storage security in cloud computing."IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON):1-4.

[10] Ahmed Albugmi, Madini O. Alassafi, Robert Walters and Gary Wills. (2016) "Data security in cloud computing."Fifth International Conference on Future Generation Communication Technologies (FGCT): 55-59.

[11] P Srikanth, Abhinav Mehta, Neha Yadav, Sahil Singh and Shubham Singhal. (2017) "Encryption and Decryption Using Genetic Algorithm Operations and Pseudorandom Number." IJCSN - International Journal of Computer Science and Network 6(3):455-459.

[12] Arjun Aggarwal, Abhijeet Mishra, Gaurav Singhal and Sushil Kr Saroj. (2016) "An Efficient Methodology for Storing Sensitive Datausing Nested Cloud."International Journal of Computer Applications 142 (10): 0975 – 8887.